NetCamera NVW IP Security Wireless Night Vision Camera

A02-IPCAM4-W54

MANUALE COMPLETO

A02-IPCAM4-W54_MI01

Where solutions begin

ISO 9001:2000 Certified Company

ITALIANO

Questo prodotto è coperto da garanzia Atlantis Land **Fast-Swap** della durata di 3 anni. Per maggiori dettagli in merito o per accedere alla documentazione completa in Italiano fare riferimento al sito **www.atlantis-land.com.**

ENGLISH

This product is covered by Atlantis Land 3 years **Fast-Swap** warranty. For more detailed informations please refer to the web site **www.atlantis-land.com.**
For more detailed instructions on configuring and using this device, please refer to the online manual.

FRANCAIS

Ce produit est couvert par une garantie Atlantis Land **Fast-Swap** de 3 ans. Pour des informations plus détaillées, référez-vous svp au site Web **www.atlantis-land.com.**

DEUTSCH

Dieses Produkt ist durch die Atlantis Land 3 Jahre **Fast-Swap** Garantie gedeckt. Für weitere Informationen, beziehen Sie sich bitte auf Web Site **www.atlantis-land.com.**

ESPAÑOL

Este producto esta cubierto por Atlantis Land con una garantía **Fast-Swap** de 3 años. Para mayor información diríjase a nuestro sitio Web **www.atlantis-land.com.**

The award of the information is facultative, but its lack will prevent ATLANTIS LAND® from starting the Guarantee process requested.

Register your product!

www.atlantis-land.com

Registration on the web site **www.atlantis-land.com** within 15 days from the purchase of the product dismiss the customer from showing a valid proof of purchase (Sale Receipt or Invoice) in case of the request of intervention. For further information we invite you to look at our web site at the section WARRANTY.

INDICE

A02-IPCAM4-W54_MI01(V1.0 Dicembre 2006)

AVVERTENZE
Abbiamo fatto di tutto al fine di evitare che nel testo, nelle immagini e nelle tabelle presenti in questo manuale, nel software e nell'hardware fossero presenti degli errori. Tuttavia, non possiamo garantire che non siano presenti errori e/o omissioni. Infine, non possiamo essere ritenuti responsabili per qualsiasi perdita, danno o incomprensione compiuti direttamente o indirettamente, come risulta dall'utilizzo del manuale, software e/o hardware.
Il contenuto di questo manuale è fornito esclusivamente per uso informale, è soggetto a cambiamenti senza preavviso (a tal fine si invita a consultare il sito www.atlantisland.it o www.atlantis-land.com per reperirne gli aggiornamenti) e non deve essere interpretato come un impegno da parte di Atlantis Land spa che non si assume responsabilità per qualsiasi errore o inesattezza che possa apparire in questo manuale. Nessuna parte di questa pubblicazione può essere riprodotta o trasmessa in altra forma o con qualsiasi mezzo, elettronicamente o meccanicamente, comprese fotocopie, riproduzioni, o registrazioni in un sistema di salvataggio, oppure tradotti in altra lingua e in altra forma senza un espresso permesso scritto da parte di Atlantis Land spa. Tutti i nomi di produttori e dei prodotti e qualsiasi marchio, registrato o meno, menzionati in questo manuale sono usati al solo scopo identificativo e rimangono proprietà esclusiva dei loro rispettivi proprietari.
Restrizioni di responsabilità CE/EMC
Il prodotto descritto in questa guida è stato progettato, prodotto e approvato in conformità alle regole EMC ed è stato certificato per non avere limitazioni EMC.
Se il prodotto fosse utilizzato con un PC non certificato, il produttore non garantisce il rispetto dei limiti EMC. Il prodotto descritto è stato costruito, prodotto e certificato in modo che i valori misurati rientrino nelle limitazioni EMC. In pratica, ed in particolari circostanze, potrebbe essere possibile che detti limiti possano essere superati se utilizzato con apparecchiature non prodotte nel rispetto della certificazione EMC. Può anche essere possibile, in alcuni casi, che i picchi di valore siano al di fuori delle tolleranze. In questo caso l'utilizzatore è responsabile della "compliance" con i limiti EMC. Il Produttore non è da ritenersi responsabile nel caso il prodotto sia utilizzato al di fuori delle limitazioni EMC.
CE Mark Warning
Questo dispositivo appartiene alla classe B. In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.
ATTENZIONE
Lasciare almeno 30cm di distanza tra le antenne del dispositivo e l'utilizzatore.

Dichiarazione di Conformità

Questo dispositivo è stato testato ed è risultato conforme alla direttiva 1999/5/CE del parlamento Europeo e della Commissione Europea, a proposito di apparecchiature radio e periferiche per telecomunicazioni e loro mutuo riconoscimento. Dopo l'installazione, la periferica è stata trovata conforme ai seguenti standard: EN 300.328(radio), EN 301 489-1, EN 301 489-17(compatibilità elettromagnetica) ed EN 60950(sicurezza). Questa apparecchiatura può pertanto essere utilizzata in tutti i paesi della Comunità Economica Europea ed in tutti i paesi dove viene applicata la Direttiva 1999/5/CE, senza restrizioni eccezion fatta per:

Francia:

Se si utilizza all'aperto tale dispositivo, la potenza in uscita è limitata (potenza e frequenza) in base alla tabella allegata. Per informazioni ulteriori consultare *www.art-telecom.fr.*

Luogo	Banda di Frequenze(MHz)	Potenza (EIRP)
Chiuso (senza restrizioni)	2400-2483,5	100mW(20dBm)
Aperto	2400-2454 2454-2483,5	100mW(20dBm) 10mW(10dBm)

Se l'uso di questa apparecchiatura in ambienti domestichi genera interferenze, è obbligo dell'utente porre rimedio a tale situazione.

Italia:

Questa periferica è conforme con l'Interfaccia Radio Nazionale e rispetta i requisiti sull'Assegnazione delle Frequenze. L'utilizzo di questa apparecchiatura al di fuori di ambienti in cui opera il proprietario, richiede un'autorizzazione generale. Per ulteriori informazioni si prega di consultare: *www.comunicazioni.it.*

Capitolo 1

Introduzione

Questo manuale è stato pensato per un utilizzo avanzato della NetCamera NVW, per questo sono stati trattati con dovizia di particolari una moltitudine di argomenti che potrebbero, almeno inizialmente, essere di difficile comprensione.
Per una configurazione rapida è comunque disponibile una Guida all'Installazione Rapida presente sia su CDRom che su supporto cartaceo a corredo del prodotto. E' inoltre disponibile, sempre sul CDRom allegato, una guida all'installazione multimediale.

1.1 Panoramica della NetCamera NVW

NetCamera NVW rappresenta la soluzione ideale per inviare video, per la videosorveglianza remota o la trasmissione di immagini in tempo reale su Internet o Intranet.
NetCamera NVW è dotata di una potente CPU, basata su un sistema operativo Linux, che la rende un sistema completamente autonomo capace di generare video MPEG4 a 30 fps in VGA e gestire autonomamente la rilevazione automatica del movimento.
Completano la dotazione l'integrazione di un microfono per la cattura di rumori e avanzate funzioni di commutazione (2x DI in ingresso, 1x DO in uscita) che rendono possibili la ricezione/invio di segnali ad altri dispositivi di allarme (rilevatori volumetrici, PIR o sirene).
NetCamera NVW integra 8 IR LEDs, e permette pertanto di riprodurre vivaci immagini a colori di giorno e nitide riproduzioni in bianco e nero di notte.
Queste caratteristiche la rendono lo strumento ideale per il monitoraggio/videosorveglianza remoti sia diurna che notturna.
NetCamera NVW può essere collegata, tramite il cavo di rete, direttamente alla LAN [un'interfaccia wireless in standard IEEE802.11g con supporto dei più elevati standard di sicurezza è inclusa] ed essere gestita e controllata anche da remoto, in maniera semplice ed intuitiva, tramite un PC o portatile collegato in Internet (o Intranet) utilizzando un qualsiasi browser web in qualunque momento e luogo.

1.2 Requisiti di sistema

Prima di procedere con l'installazione del prodotto verificare di disporre dei seguenti requisiti:

- Local Area Network: 10Base-T Ethernet oppure 100Base TX Fast Ethernet
- CPU: Intel Celeron 1.5GHz o superiore (Intel Pentium 4 consigliato)
- Memoria: 128 MB (sono raccomandati 256 MB)
- VGA card resolution: 800x600 o Superiore
- Internet Explorer 5.0 or above (ActiveX)

1.3 Contenuto della confezione

Una volta aperta la confezione dovrebbero essere presenti i seguenti accessori:

- Atlantis Land NetCamera NVW
- Guida di Quick Start
- CDRom contenente il manuale
- Kit (incluso di viti) per il fissaggio a muro
- Cavo CAT-5 LAN
- Alimentatore (5V, 2A)

Qualora mancasse qualcosa consultare immediatamente il rivenditore.

Capitolo 2

Uso della NetCamera NVW

2.1 Precauzioni nell'uso della NetCamera NVW

Seguire i seguenti accorgimenti per un corretto utilizzo dell'apparato.

Non usare il dispositivo in un luogo in cui ci siano condizioni di alte temperatura ed umidità, l'apparato potrebbe funzionare in maniera impropria e danneggiarsi.
Non usare la stessa presa di corrente per connettere altri apparecchi al di fuori della NetCamera NVW.
Non aprire mai il case della NetCamera NVW né cercare di ripararlo da soli.
Se la NetCamera NVW dovesse essere troppo calda, spegnerla immediatamente e rivolgersi a personale qualificato.
Non appoggiare il dispositivo su superfici plastiche o in legno che potrebbero non favorire lo smaltimento termico (nel caso non si usasse il piedistallo).
Usare il dispositivo solo ed esclusivamente in ambienti indoor.

Assicurarsi che il piedistallo sia ben bloccato alla parete, al fine di evitare la caduta e la probabile rottura della NetCamera NVW.
Usare esclusivamente l'alimentatore fornito nella confezione, l'uso di altri alimentatori farà automaticamente decadere la garanzia.
Non effettuare upgrade del firmare utilizzando l'interfaccia wireless ma solo quella wired. Questo potrebbe danneggiare il dispositivo ed invalidare la garanzia.

2.2 I LED frontali

Lens Assembly

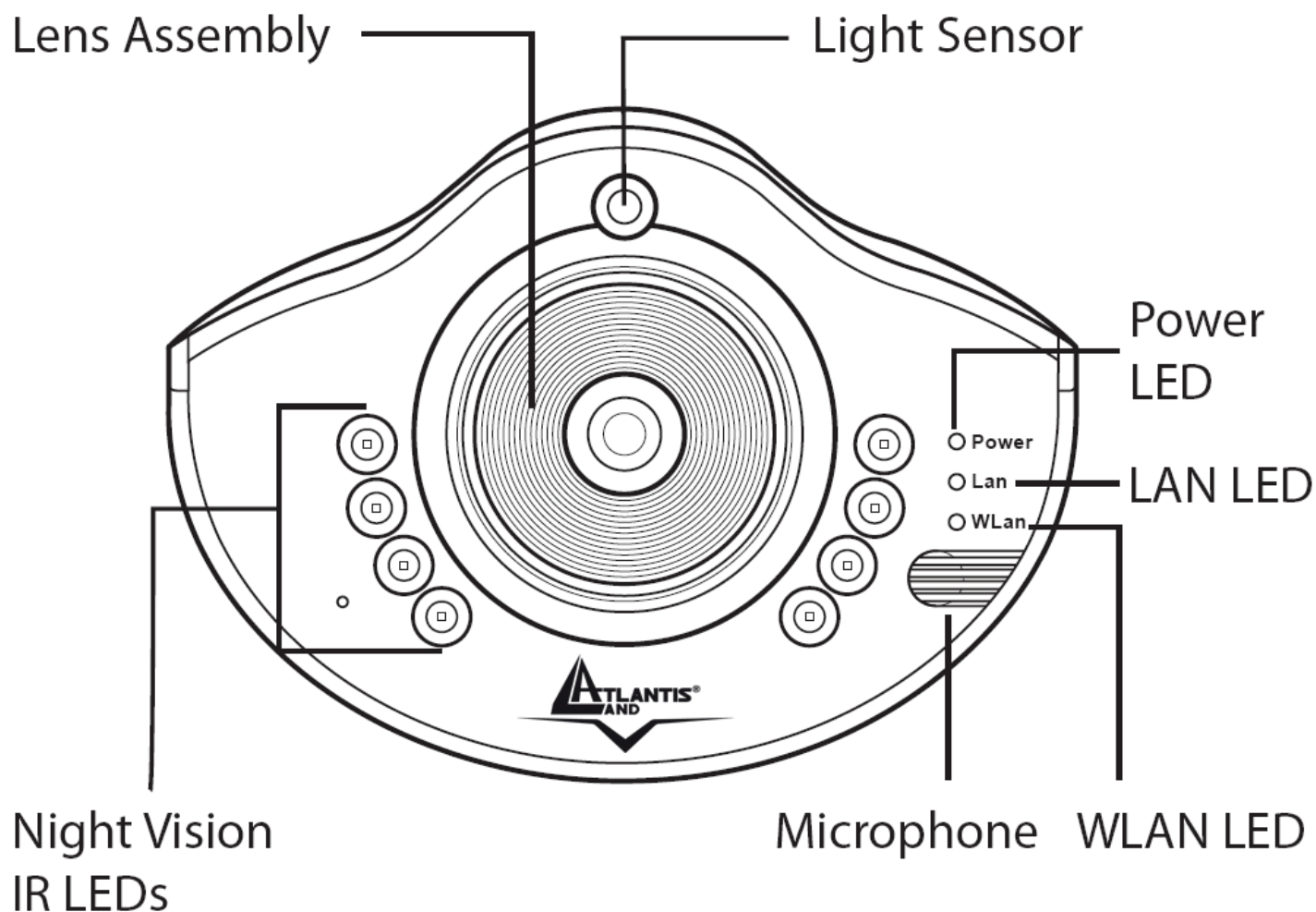
Light Sensor

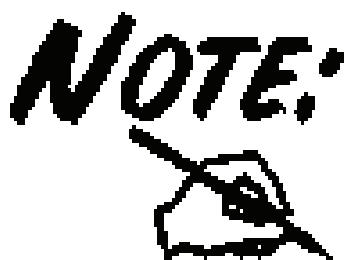
Power LED

LAN LED

Night Vision IR LEDs

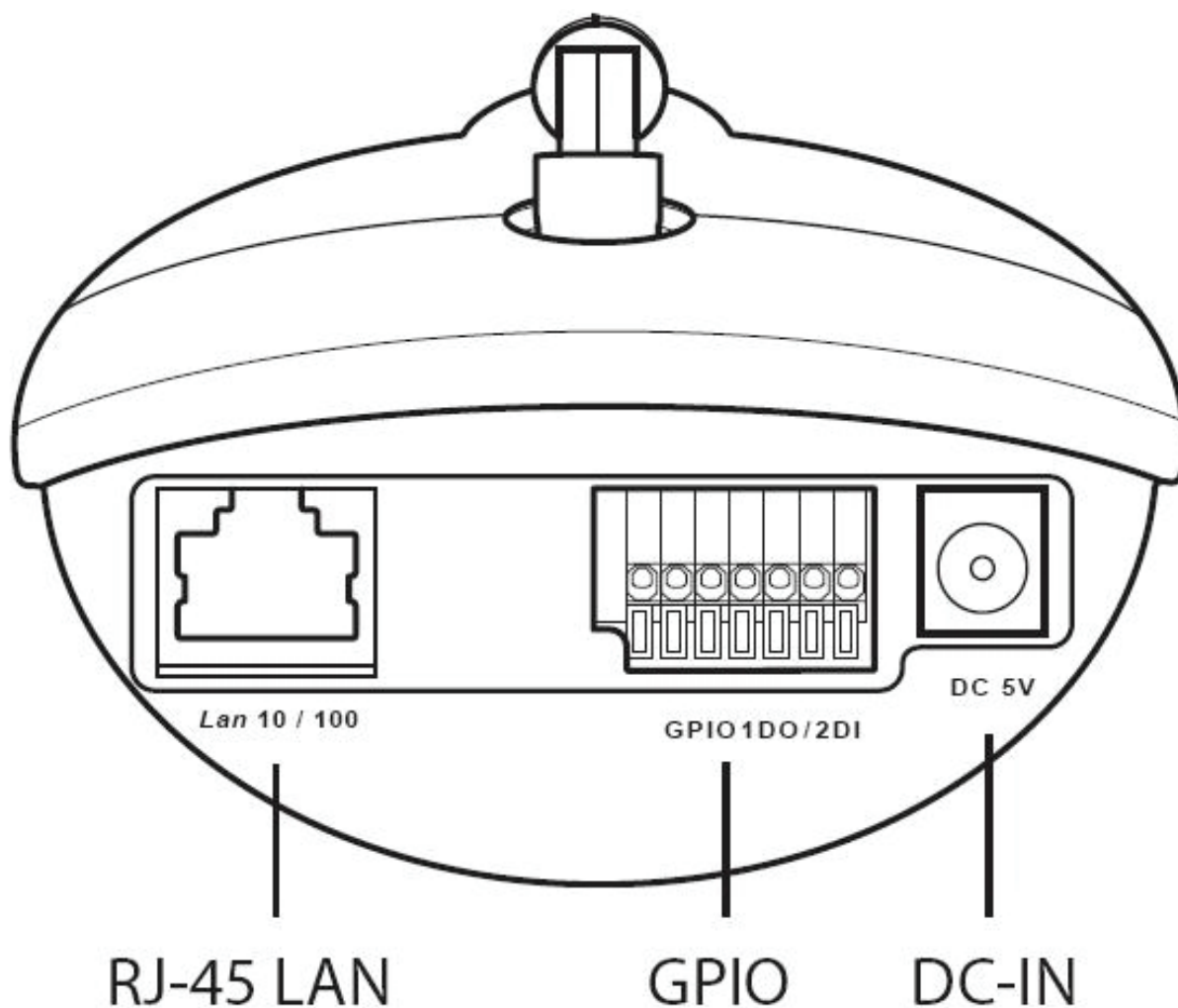
Microphone

WLAN LED

LED	Informazione
Power	Acceso verde fisso indica il corretto collegamento del dispositivo alla rete elettrica
Lan	Acceso Fisso= connessione attiva Lampeggiante quando vi è trasmissione/ricezione
WLan	Acceso Fisso= connessione wireless attiva Lampeggiante quando vi è trasmissione/ricezione

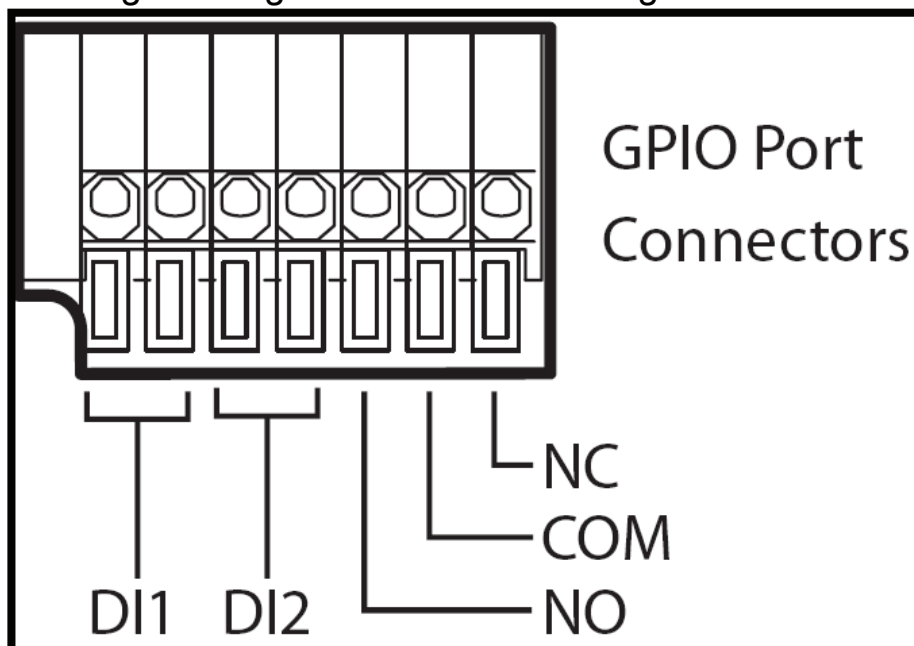
Night Vision	Gli 8 Led Infrarossi permettono al dispositivo una chiara visione notturna
Light Sensor	Sensore di luminosità (non ostruire il alcun modo)
Microphone	Microfono per catturare il rumore d'ambiente

L'utilizzo di dispositivi in grado di catturare immagini, video o voce potrebbero essere regolamentati o completamente proibiti in talune giurisdizioni. Potrebbe essere richiesta un'autorizzazione.
Atlantis Land SpA non garantisce in alcun modo che I propri prodotti siano utilizzati in conformità con le leggi locali ed inoltre non può essere ritenuta responsabile per un uso improprio di tali dispositivi.

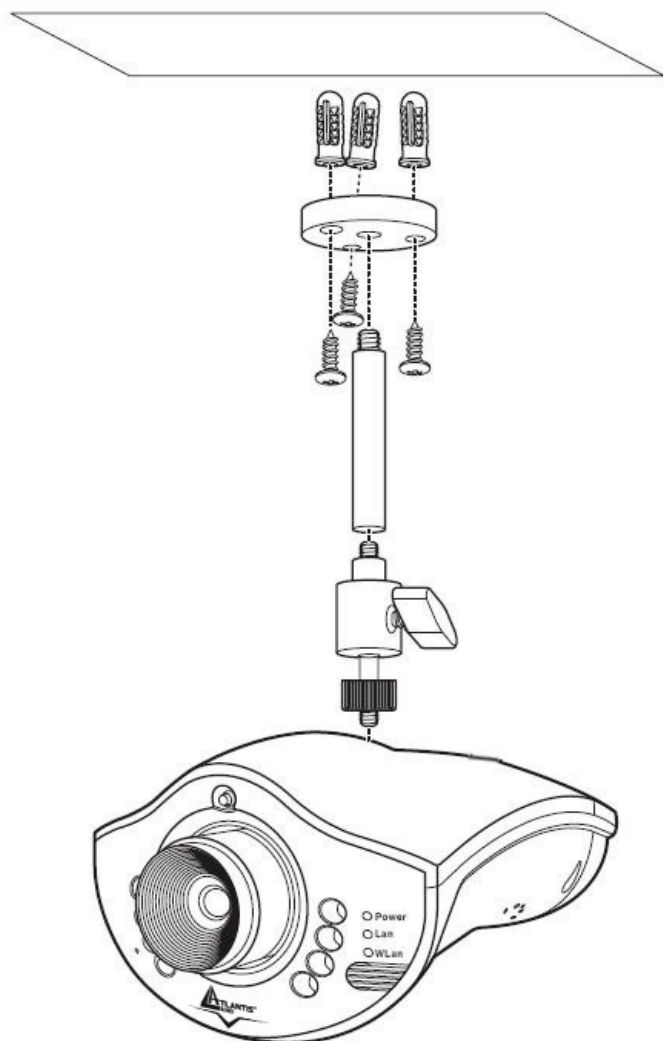
2.3 Le porte posteriori

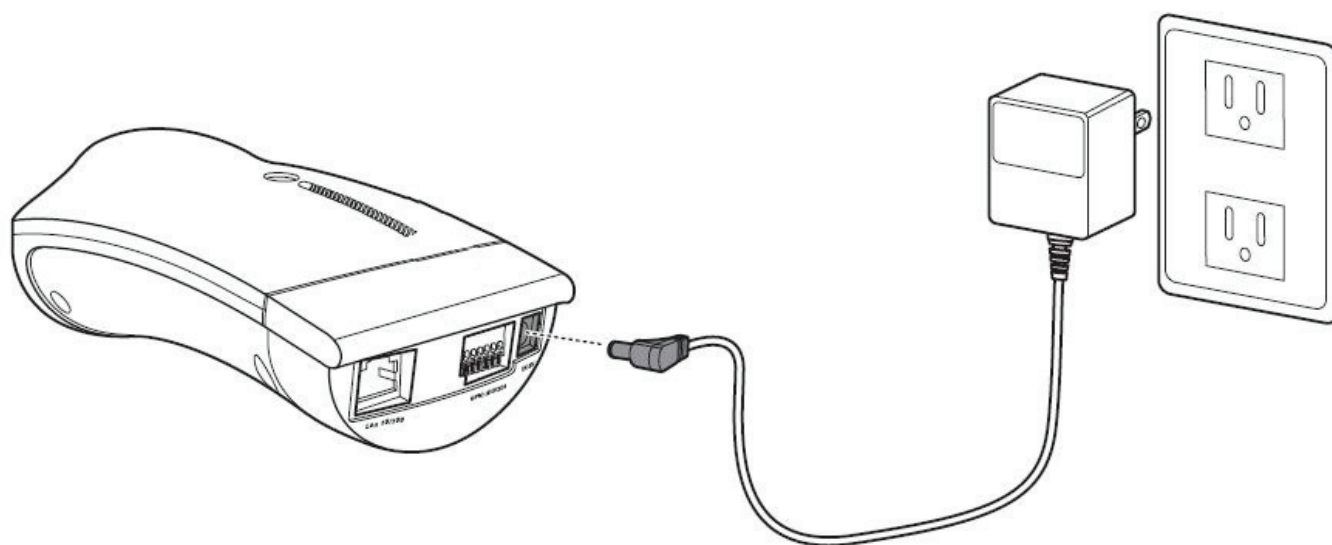
Lan 10 / 100
GPIO1DO/2DI
DC 5V

RJ-45 LAN GPIO DC-IN

Porte	Utilizzo
Network Cable	Connettere il cavo RJ-45 a questa porta per effettuare l'allacciamento alla Lan
GPIO Connectors	Sono disponibili due ingressi digitali ed un interruttore controllato.

DC-IN	Connettere l'alimentatore incluso a questo jack ed alla rete elettrica

Nella figura allegata è illustrato il dettaglio dei contatti DI/DO.

2.4 Cablaggio

NetCamera NVW può essere assemblata in 2 modalità differenti. Il piedistallo può essere agganciato tanto alla parte superiore che inferiore della NetCamera NVW. Collegare il piedistallo alla NetCamera NVW seguendo le illustrazioni e, utilizzando le viti incluse, fissarla ad una superficie stabile (muro). Il piedistallo, una volta fissato alla parete, permette il puntamento dell'ottica verso qualsiasi direzione.

Non collocare la NetCamera NVW in ambienti esterni e/o in ambienti ove potrebbe essere esposta ad agenti atmosferici. Assicurarsi che il piedistallo sia saldamente ancorato alla parete (al fine di evitare che la NetCamera NVW possa cadere).

Collegare l'alimentazione esterna alla presa DC che si trova sul pannello posteriore della webcamera, e poi collegare alla rete elettrica l'alimentatore e controllare che il LED di alimentazione (Power) sulla webcamera sia acceso.

Collegare il cavo ethernet al connettore per il cavo di rete che si trova nel pannello posteriore della webcamera e poi collegarlo alla rete LAN.

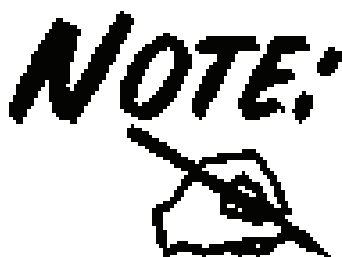
NOTE: Utilizzare esclusivamente l'adattatore fornito nella confezione.

Capitolo 3

Prima di iniziare

La NetCamera NVW può essere configurata via browser Web che dovrebbe essere incluso nel Sistema Operativo o comunque facilmente reperibile in Internet. Il prodotto offre una semplice interfaccia di configurazione.

3.1 Prima di iniziare

Questa sezione descrive la configurazione richiesta dai singoli PC connessi alla LAN cui è collegato il dispositivo. Tutti i PC devono avere una scheda di rete Ethernet o Adattatore Wireless installata correttamente, essere connessi alla NetCamera NVW direttamente o tramite un Hub/Switch o in Wireless ed avere il protocollo TCP/IP installato e correttamente configurato. L'indirizzo IP, normalmente appartenente ad una classe privata, deve essere nella classe 192.168.1.x con Subnet 255.255.255.0. Anzitutto è necessario preparare i PC inserendovi (qualora non vi fosse già) la scheda di rete / Adattatore Wireless. E' necessario poi installare il protocollo TCP/IP. Qualora il TCP/IP non fosse correttamente configurato, seguire gli steps successivi:

Qualsiasi workstation col TCP/IP può essere usata per comunicare con o tramite la NetCamera NVW. Per configurare altri tipi di workstations fare riferimento al manuale del produttore.

3.1.1 Configurazione del PC in Windows 95/98/ME

1. Andare in Start/Settings/Control Panel. Cliccare 2 volte su Network e scegliere Configuration.

2. Selezionare TCP/IP ->NIC Compatible, o qualsiasi Network Interface Card (NIC) del PC.

3. Cliccare su Properties.

4. Selezionare l’opzione Specify an IP address (dopo aver scelto IP Address) ed introdurre un indirizzo IP del tipo 192.168.1.X (X compreso tra 2 e 254 escluso 1 che è l’IP utilizzato dalla NetCamera NVW)e subnet mask 255.2552.255.0.
5. Andare su DNS Configuration

6. Selezionare l’opzione Enable DNS ed introdurre l’indirizzo IP del DNS (chiedere tale informazione al proprio ISP).

3.1.2 Configurazione del PC in Windows NT4.0

1. Andare su Start/Settings/ Control Panel. Cliccare per due volte su Network e poi cliccare su Protocols.

2. Selezionare TCP/IP Protocol e poi cliccare su Properties.

3. Selezionare l’opzione Specify an IP Address e ed introdurre un indirizzo IP del tipo 192.168.1.x (X compreso tra 2 e 254 escluso 1 che è l’IP utilizzato dalla NetCamera NVW) e subnet mask 255.255.255.0. Premere OK per terminare.

3.1.3 Configurazione del PC in Windows 2000

1. Andare su Start/Settings/Control Panel. Cliccare due volte su Network and Dial-up Connections.
2. Cliccare due volte su Local Area Connection.
3. In Local Area Connection Status cliccare Properties.
4. Selezionare Internet Protocol (TCP/IP) e cliccare su Properties
5. Selezionare l'opzione Use the Following IP address ed introdurre un indirizzo IP del tipo 192.168.1.X (X compreso tra 2 e 254 escluso 1 che è l'IP utilizzato dalla NetCamera NVW) e subnet mask 255.255.255.0.
6. Successivamente scegliere Use the Following DNS server address (chiedere tale informazione al proprio ISP) ed introdurre l'indirizzo IP dei server DNS.
7. Premere su OK per terminare la configurazione

3.1.4 Configurazione del PC in Windows XP

1. Andare su Start e poi Control Panel. Cliccare due volte su Network (in Classic View) Connections.
2. Cliccare due volte su Local Area Connection.
3. In Local Area Connection Status cliccare Properties.
4. Selezionare Internet Protocol (TCP/IP) e cliccare su Properties.
5. Selezionare l'opzione Use the following IP address ed introdurre un indirizzo IP del tipo 192.168.1.x (X compreso tra 2 e 254 escluso 1 che è l'IP utilizzato dalla NetCamera NVW)e subnet mask 255.255.255.0.
6. Successivamente Use the following DNS server addresses (chiedere tale informazione al proprio ISP) ed introdurre l'indirizzo IP dei server DNS.
7. Premere su OK per terminare la configurazione.

3.1.5 Verifica della Configurazione

Per verificare il successo della configurazione (dopo aver riavviato il PC, operazione necessaria su Win98, 98Se,ME e invece sufficiente ottenere il rilascio dell'IP su XP, 2000), utilizzare il comando ping. Da una finestra Dos digitare:
ping 192.168.1.1
Se appare il seguente messaggio:

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 times<10ms TTL=64
Reply from 192.168.1.1: bytes=32 times<10ms TTL=64
Reply from 192.168.1.1: bytes=32 times<10ms TTL=64

E' possibile procedere andando al punto seguente. Se invece appare il seguente messaggio:

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Controllare che il led LAN /Wireless sia acceso (cambiare il cavo qualora non fosse così). Controllare l'indirizzo del PC digitando winipcfg per (Win95,98,ME) o ipconfig (per Win2000,XP) ed eventualmente reinstallare lo stack TCP/IP.

3.2 Settaggi di Default

Prima di iniziare la configurazione della NetCamera NVW è necessario conoscere quali siano i settaggi di default:

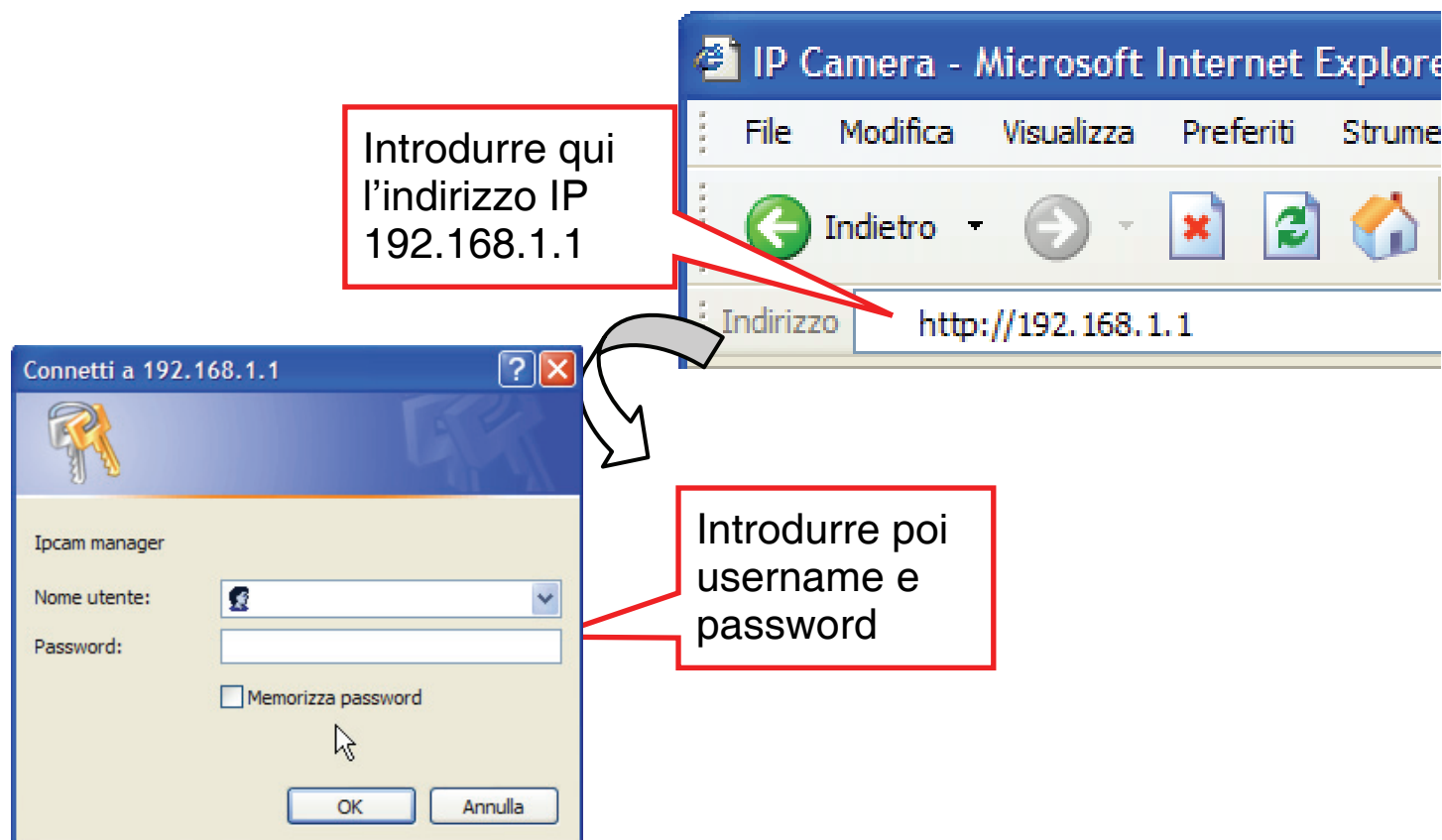
- Nome Utente: **admin**
- Password: **atlantis**
- Indirizzo IP (**192.168.1.1**)
- Subnet Mask(**255.255.255.0**)
- **Wireless:**
    - Connection Type=Infra
    - Contry Region=ETSI(Europe)
    - Channel=6

- SSID(ESSID)=NetCameraNVW

3.3 Configurazione IP Security Night Vision Cam

Accedere col browser web al seguente indirizzo IP che di default è: http://192.168.1.1, e premere il tasto invio.

Introdurre qui l'indirizzo IP 192.168.1.1

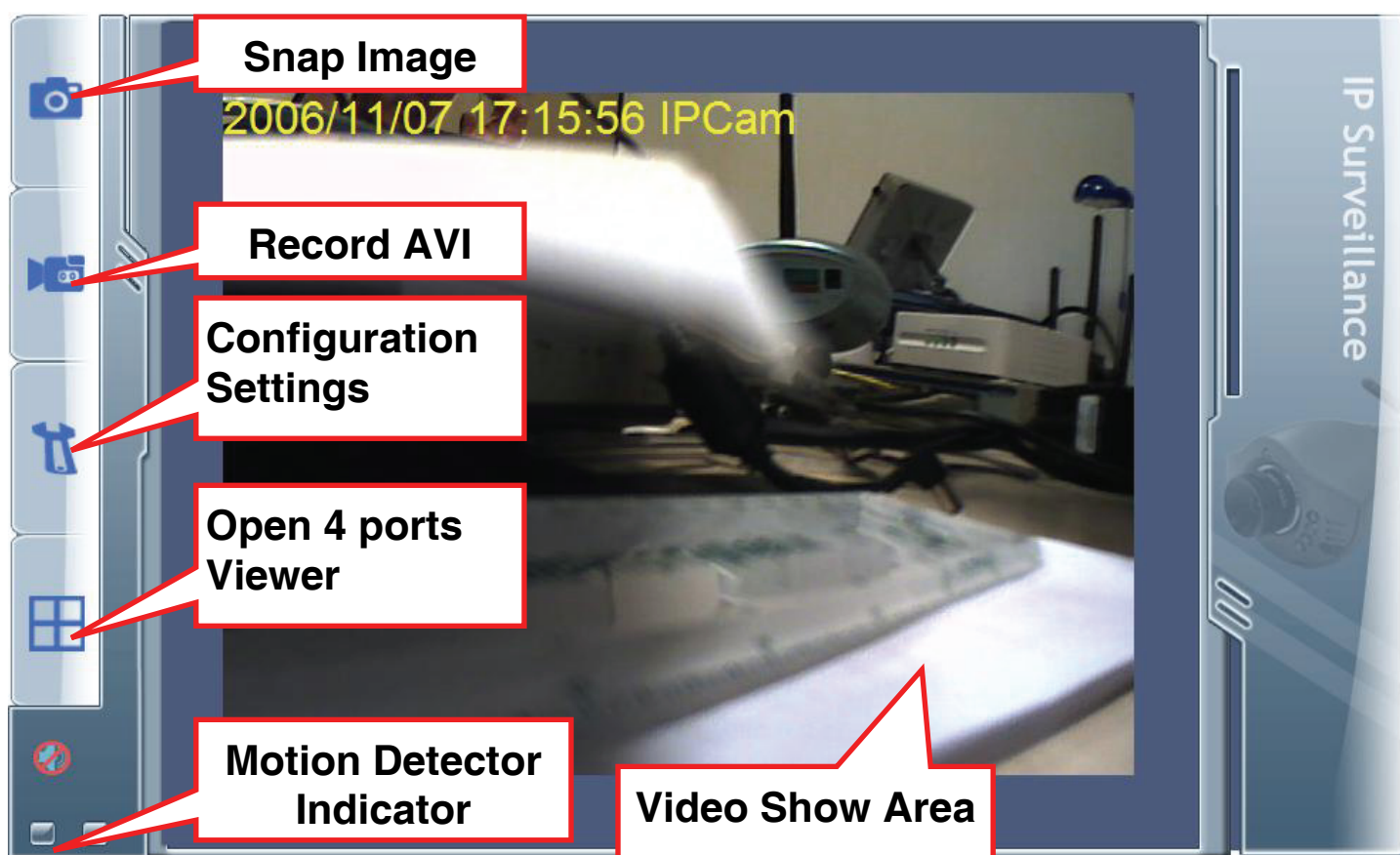
Introdurre poi username e password

Apparirà a questo punto il Menù Principale diviso in 3 differenti aree: Menu Bar, Video Show Area e Control Buttons.

A questo punto, alla prima apertura del browser, potrebbe essere necessario installare un controller ActiveX. Tale installazione è obbligatoria.

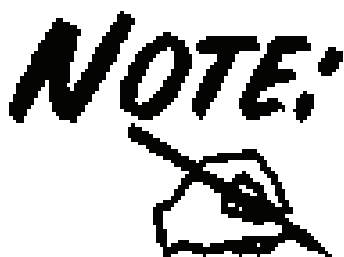
- Immediatamente sotto l'indirizzo http potrebbe apparire la scritta: **Questo Sito potrebbe richiedere il seguente controllo ActiveX: ´*ATL3.0:VCView*´ da ´Atlantis Land SpA ´. Fare clic qui per procedere con l'intallazione…**

- Ciccarci sopra col tasto destro e scegliere **Installa Controllo ActiveX**
- Cliccare nuovamente su **Installa** nella finestra.

Il Video Live può adesso essere visto nel browser.

Snap Image
2006/11/07 17:15:56 IPCam
Record AVI
Configuration Settings
Open 4 ports Viewer
Motion Detector Indicator
Video Show Area
IP Surveillance

Cliccando su:

- **Snap Image**: Permette di salvare, in formato JPG, l'immagine a video. Per modificare la directory dove il file viene salvato consultare il capitolo seguente (4.1.4).
- **Record AVI**: Permette di creare un file AVI con un frame rate predefinito. Durante la registrazione il bottone diventerà di colore rosso. Per interrompere la registrazione cliccare nuovamente sull'icona. Per modificare la directory dove il file video viene salvato consultare il capitolo seguente (4.1.4).

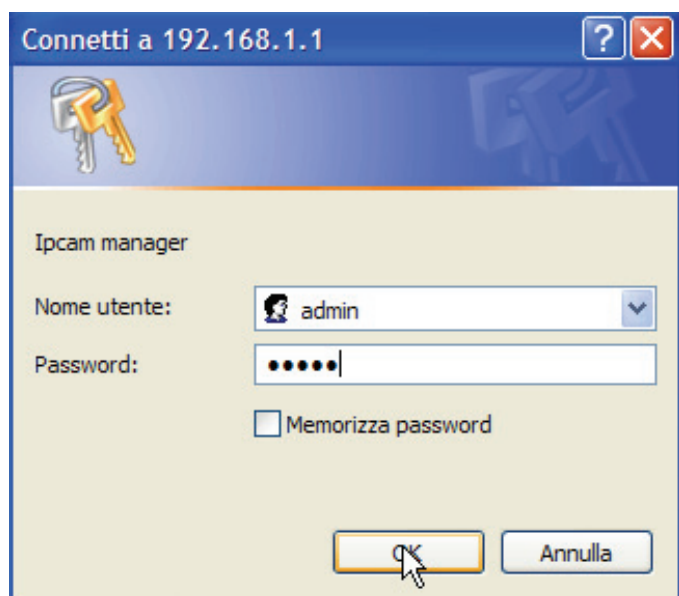
- **Configuration Settings**: E' possibile controllare il dispositivo in ogni dettaglio. Consultare il capitolo seguente.
- **Open 4 ports View**: E' possibile accedere direttamente ad altre NetCamera NVW (precedentemente configurate).

Il PC da cui si effettua la configurazione deve avere un IP nella stessa classe della NetCamera NVW (esempio 192.168.1.2 e subnet mask=255.255.255.0)

Capitolo 4

Configurazione avanzata tramite Browser

In questo capitolo è possibile effettuare la configurazione avanzate del dispositivo.
Accedere col browser web al seguente indirizzo IP (dove solitamente si inserisce l'URL) che di default è: **192.168.1.1**, e premere poi il tasto invio.
Una volta entrati nella configurazione via web (si veda il capitolo precedente), cliccare sull'icona **Configuration Settings** (posta nella barra degli strumenti nella zona sinistra).

Il dispositivo chiederà l'immissione della password di accesso.

Immettere l'username e la password (utilizzare **admin** per username e **atlantis** come password, nel caso di primo accesso). Qualora la password fosse stata cambiata inserire quella memorizzata nel dispositivo. Premere **OK** per continuare.

Si raccomanda, una volta configurato il dispositivo di cambiare la password di accesso.

Apparirà a questo punto il Menù Principale, nella cui parte sinistra sono contenute 3 Icone.

System
Home
Basic
Advanced
Network
User
Video
Video Player
BASIC SETTING

Per tornare alla schermata principale

Per accedere alla configurazione

Per accedere alla configurazione Avanzata

Camera Name IPCam-5C24 Save

LAN IP Address 192.168.1.186
LAN Netmask Address 255.255.255.0
LAN Gateway Address 192.168.1.6
DHCP State Disabled

Wireless Status
Connection DOWN
Channel 1
Signal Level 0%
TX Rate 54Mbps

Cliccando sulla sezione desiderata appariranno tutti i settaggi relativi alla configurazione della sezione scelta.

4.1 Basic Settings

In questa sezione della NetCamera NVW è possibile controllare lo stato di funzionamento dell'apparato, cambiarne l'indirizzamento, configurarne l'accesso ed impostare la qualità delle riprese audio/video.
Cliccando sul Menù Status si apriranno tutte le seguenti sottosezioni:

- System
- Network
- User
- Video
- Video Player

Queste sottosezioni mostrano un quadro dettagliato sullo stato di funzionamento della relativa funzionalità.

4.1.1 System

Una volta cliccato il menu **System** si apriranno tutte le seguenti sottosezioni:

- Status
- Log
- Time
- Firmware

Status

In questa sezione è possibile visualizzare tutti gli stati del dispositivo ed avere così un quadro immediato dello stato di funzionamento. Sono reperibili informazioni riguardante la Camera, Configurazione LAN e WLAN.

Status | Log | Time | Firmware

Camera Information	
Firmware Version	C64000-WX-2.00.00-60728-ZZ
Camera Type	CMOS
Current Live-View Users	0
Camera Name	IPCam-5C24 Save
Ethernet Status	
Ethernet MAC Address	00-14-29-00-5C-24
LAN IP Address	192.168.1.186
LAN Netmask Address	255.255.255.0
LAN Gateway Address	192.168.1.6
DHCP State	Disabled
Wireless Status	
Connection	DOWN
Channel	1
Signal Level	0%
TX Rate	54Mbps

Log

In questa sezione è possibile controllare lo stato dei vari moduli e componenti dell'apparato.

Status | Log | Time | Firmware

Log List

Time	Event
001 11:20:18 11/16/2006	Connect to LiveView
002 10:29:07 11/16/2006	guest login in from 192.168.1.185
003 10:29:06 11/16/2006	admin login in from 192.168.1.185
004 10:26:52 11/16/2006	guest login in from 192.168.1.185
005 10:26:51 11/16/2006	admin login in from 192.168.1.185
006 10:16:43 11/16/2006	guest login in from 192.168.1.185
007 10:16:42 11/16/2006	admin login in from 192.168.1.185
008 10:16:11 11/16/2006	Connect to LiveView
009 10:16:06 11/16/2006	guest login in from 192.168.1.185
010 09:39:54 11/16/2006	guest login in from 192.168.1.185

Clear | PrePage | NextPage

Cliccare su **Clear** per cancellare i log memorizzati.
Cliccare su **PrePage/NextPage** per indietreggiare/avanzare di pagina.

Time

Il dispositivo non ha un orologio al suo interno, usa il protocollo SNTP per risolvere tale inconveniente.

Status | Log | Time | Firmware

Current Camera Time

Date: 2006-11-16 Time: 12:32:14 Refresh

NTP Configuration

☑ Synchronize with Time server

Time Zone GMT+01 (Amsterdam, Berlin, Rome, Stockholm)

NTP server pool.ntp.org

Save

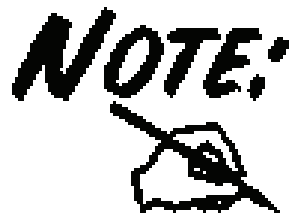
Manually Update Camera Time

Synchronize with computer time

Date: 2006-11-16 Time: 12:32:16 Update

Set manually

Date: 2006-11-16 Time: 12:31:59 Update

Nella sezione **Current Camera Time** è possibile visualizzare l'impostazione temporale utilizzata dalla NetCamera NVW. Cliccare su **Refresh** per forzare l'aggiornamento.
Nella sezione **NTP Configuration** è invece possibile impostare il server SNTP per la rcezione automatica della data/ora. Anzitutto attivare tale funzionalità spuntando la voce **Synchronize with Time server**, poi scegliere la zona di appartenenza (nella combo-box **Time Zone**) e infine cliccare su **Save** per rendere permanenti i settaggi. E' possibile ricevere, pertanto, l'ora e data corretta solo dopo che il collegamento ad Internet è attivo.

In caso di problemi utilizzare i seguenti settaggi:
NTP Server=pool.ntp.org oppure **128.138.140.44**
Cliccare, dopo 1 minuto circa, su **Save** per attivare la sincronizzazione.
I campi **Date** e **Time** dovrebbero aggiornarsi.

Nella sezione **Manually Update Camera Time** è possibile è possibile sincronizzare i parametri di data e ora della NetCamera NVW con quelli del computer (da cui si effettua l'accesso) oppure impostare manualmente la data/ora. Cliccare poi su **Update** per aggiornare l'apparato.

Firmware

Nella sezione **Maintain Camera** è possibile effettuare il riavvio della telecamera (cliccare su **Restart**) , il reset alle condizioni iniziali (cliccare su **Default**) oppure un reset alle condizioni iniziali eccetto l'indirizzo IP (cliccare su **Restore**).

Status | Log | Time | Firmware

Maintain Camera

Restart — Restart camera.

Restore — Reset all parameters, except IP address configuration, to original factory settings.

Default — Reset all parameters to original factory settings.

Upgrade Firmware

Current version: C64000-WX-2.00.00-60728-ZZ

Warning: Do not unplug camera power while upgrading.

Specify the firmware file to upgrade:

[ ] Sfoglia... and click Upgrade

It will restart automatically after 2 minutes.

Nella sezione Upgrade Firmware è invece possibile aggiornare il firmware della NetCamera NVW. Per effettuare l'upgrade è anzitutto necessario scaricare dal sito www.atlantisland.it o www.atlantis-land.com (nella sezione opportuna) un nuovo firmware (se disponibile). Aprire il file compresso in una directory. Cliccare su **Sfoglia** ed indicare la path contenente il firmware decompresso. Premere poi sul tasto **Upgrade** per terminare l'aggiornamento.

E' opportuno garantire, durante l'intera fase di upgrade, alla NetCamera NVW l'alimentazione elettrica. Qualora questa venisse a mancare il dispositivo potrebbe non essere recuperabile.

Verificare che solo un cavo ethernet sia connesso (quello del PC da cui si effetua l'upgrade).

Effettuare l'upgrade utilizzando una connessione wired e non wireless. Questo potrebbe danneggiare il dispositivo ed invalidare così la garanzia.

Durante la procedura di upgrade è opportuno non chiudere il browser Web, caricare nuove pagine o cliccare su link. Questo potrebbe danneggiare il firmware e rendere inusabile il dispositivo.

Durante la fase di upgrade il dispositivo indicherà lo stato di completamento della riscrittura del firmware mostrando un indicatore percentuale.

4.1.2 Network

Una volta cliccato il menu **NetWork** si apriranno tutte le 4 seguenti sottosezioni:

- Ethenet
- Wireless
- PPPoE
- Dynamic DNS

Ethernet

Nella sezione **IP Configuration** è possibile impostare la modalità con cui il dispositivo ottiene l'indirizzo IP.
Spuntare **Obtain IP Address via DHCP** se sulla rete è presente un server DHCP. Cliccare su **View** per visualizzare l'indirizzo IP assegnato alla NetCamera NVW.
Spuntare **Use the following IP Address** per impostare manualmente l'indirizzo IP alla NetCamera NVW. In questo caso riempire i campi **IP Address, Subnet Mask** e **Default Gateway.**

Ethernet | Wireless | PPPoE | DDNS

IP Configuration

○ Obtain IP address via DHCP [View]
⦿ Use the following IP address:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.6

DNS Configuration

○ Obtain DNS server address via DHCP [View]
⦿ Use the following DNS server address:

Primary DNS server	192.168.1.211
Secondary DNS server	

HTTP Port

HTTP port: 80

[Save] [Reload]

Nella sezione **DNS Configuration** è possibile impostare la modalità con cui il dispositivo ottiene l'indirizzo IP dei server DNS.
Spuntare **Obtain DNS Address via DHCP** se sulla rete eè presente un server DHCP. Cliccare su **View** per visualizzare l'indirizzo IP assegnato alla NetCamera NVW.

Spuntare **Use the following DNS server Address** per impostare manualmente l'indirizzo dei server DNS utilizzati dalla NetCamera NVW. In questo caso riempire i campi **Primari DNS Server** e **Secondary DNS Server.**
Nella sezione **http Port** è invece possibile impostare la porta di configurazione della NetCamera NVW.

Al fine di poter effettuare una configurazione remota della NetCamera NVW verificare quanto segue:

- sia correttamente impostato l'indirizzo IP del Default Gateway nella NetCamera NVW
- sul router ADSL sia creata una rotazione di porta opportuna sull'IP della NetCamera NVW (la stessa porta impostata nella sezione **http port**)
- nessu firewall sia abilitato sul router ADSL

Una volta effettuate le configurazioni opportune cliccare su **Save** per rendere permanenti i settaggi.

Wireless

In questa sezione è possibile effettuare le seguenti funzionalità:

- **Configuare le impostazioni wireless**
- **Impostare Sicurezza (Wireless Security Setup)**

Ethernet | Wireless | PPPoE | DDNS

Basic Configuration

Connection Type:	Infra
Country Region:	ETSI (Europe)
Channel:	6
SSID (ESSID):	NetCameraNV
Ad-Hoc Type:	802.11g 54Mbps

Security Configuration

Authentication Type:	Open System
Encryption Type:	None
WEP Key :	(5, 10, 13, 26 letters)

Save | Reload

Nella sezione **Basic Configuration** è possibile configurare le impostazioni base dell'interfaccia wireless integrata.

- **Connection Type:** A differenza delle reti LAN le reti Wireless hanno due differenti modalità di funzionamento: **infrastructure** ed **ad-hoc**. Nella configurazione Infrastructure una rete WLAN e una rete LAN comunicano tra loro tramite un access point. In una rete ad-hoc i client wireless comunicano tra loro direttamente. La scelta tra le due configurazioni è quindi dettata dalla necessità o meno di mettere in comunicazione una rete wireless con una cablata. Se i computer collegati alla rete wireless devono accedere a risorse o periferiche condivise sulla rete cablata sarà necessario utilizzare la modalità infrastructure. L' Access Point trasmetterà le informazioni ai client wireless (lin questo caso la NetCamera NVW) che potranno muoversi all'interno di un determinato raggio di azione. L'impiego contemporaneo di più Access Point permetterà di estendere l'area di copertura del segnale. I client wireless stabiliranno automaticamente il link con il dispositivo che fornisce il segnale migliore grazie alla funzionalità

roaming. Se la rete wireless ha dimensioni relativamente ridotte e se le risorse condivise sono dislocate sui personal computer che ne fanno parte, è possibile utilizzare la modalità **ad-hoc**. Questa modalità permette di collegare i client wireless tra loro direttamente senza la necessità di un access point. La comunicazione tra i client è limitata direttamente dalla distanza e dalle interferenze che intercorrono tra loro.

- **Country Region:** In questa sezione è possibile scegliere la regione in cui il dispositivo wireless verrà utilizzato. Questo, automaticamente, regolerà l'apparato nel rispetto delle regole vigenti (per l'Europa scegliere **ETSI**).
- **Channel:** Indica il canale ove l'Access Point opera. Lo standard ETSI (valido in Europa) prevede l'uso dei canali dal N°1 al N°13.
- **SSID:** Service Set Identifier, è un nome univoco condiviso da tutti i client wireless ed AP (se in roaming). Usando SSID diversi è possibile associare determinati client a determinati AP. E' una stringa ASCII composta da un massimo di 32 caratteri.
- **Ad-Hoc Type:** E' possibile far funzionare il dispositivo in modalità esclusiva (scegliendo dal menu a tendina 802.11b o 802.11g) oppure in modalità ibrida (scegliendo 802.11b+g). Selezionare la modalità operativa tra:

    1. **G and B:** permette il funzionamento con apparati IEEE802.11b ed IEEE802.11g
    2. **G Only:** permette il funzionamento esclusivamente con apparati IEEE802.11g

Nella sezione **Security Configuration** è possibile configurare le impostazioni sulla protezione usata nelle comunicazioni wireless.
Sono disponibili 3 opzioni: **Open System, Sharing Key** e **WPA-PSK.**

- **WPA-PSK**: Il protocollo Wi-Fi Protected Access (WPA) rappresenta quanto di meglio sia oggi disponibile in termini di sicurezza wireless. Nella modalità Pre-Shared Key è sufficiente impostare la Passphrase (di almeno 8 caratteri) e poi confermarla. Questa configurazione va poi ripetuta in tutti i dispositivi Wireless che accedono all'AP. L'uso del WPA, che utilizza il TKIP(Temporal Integrity Protocol), consente al dispositivo di generare le chiavi a partire dalla Passphrase e di cambiarle poi nel tempo offrendo così un alto livello di sicurezza. Il fatto di non richiedere un server RADIUS rende questa caratteristica fruibile anche per l'utente domestico o il piccolo ufficio. Nel menu **Encryption Type** scegliere

TKIP(WPA-PSK) ed introdurre nel campo **WPA-PSK** la chiave (almeno 8 caratteri). In Figura un esempio di configurazione WPA-PSK.

Ethernet | Wireless | PPPoE | DDNS

Basic Configuration

Connection Type:	Infra
Country Region:	ETSI (Europe)
Channel:	1
SSID (ESSID):	A02-AP2-W54M
Ad-Hoc Type:	802.11g 54Mbps

Security Configuration

Authentication Type:	WPA-PSK
Encryption Type:	TKIP (WPA-PSK)
WEP Key :	(5, 10, 13, 26 letters)
WPA-PSK Key :	stefanino7791

Save Reload

- **Open System:** Questo algoritmo è quello utilizzato di default. Il mittente e il destinatario non condividono le chiavi segrete per la comunicazione. Le parti generano loro stesse una coppia di chiavi e chiedono alla rispettiva controparte di accettarle. Le chiavi vengono rigenerate ogni volta che la connessione viene stabilita. Non resta che introdurre le chiavi **WEP**. Nel menu **Encryption Type** scegliere **WEP** ed introdurre nel campo **WEP-KEY** la chiave (si veda la nota esplicativa a fondo paragrafo).
- **Shared Key:** Mittente e destinatario condividono le stesse chiavi segrete, utilizzandole fino a che l'utente non decide di modificarle. Non resta che introdurre le chiavi **WEP**. Nel menu **Encryption Type** scegliere **WEP** ed introdurre nel campo **WEP-KEY** la chiave (si veda la nota esplicativa a fondo paragrafo).

Una volta effettuata la configurazione cliccare su **Save**. Il dispositivo si riavvierà automaticamente. Nella sezione **System->Status.>Wireless** Status è possibile controllare l'attività dell'interfaccia wireless.

Configurazione **WEP**: Scegliere prima il numero identificativo della chiave. Introdurre a questo punto la chiave associata.
E' possibile scegliere la lunghezza in bit [64,128] della chiave e la tipologia[STRING, HEX].

	STRING	HEX
64 bit	5*X	10*Y
128 bit	13*X	26*Y

X=[(0~9, A~Z, a~z Alphanumeric]
Y=[0~9, A~F Hexadecimal]
Ad esempio una chiave WEP da 128 bit in ASCII potrebbe essere "**atlantisland1**". [una stringa composta da 13 caratteri].
Una chiave HEX da 128 bit potrebbe essere usa stringa di 26 caratteri [0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F]

Il WEP viene oggi considerata non come assolutamente sicura e pertanto laddove possibile si consiglia l'uso del WPA.

La selezione errata della regione (nel campo Region) potrebbe portare ad un utilizzo di frequenze vietate. E' necessario scegliere la regione corretta.

Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11g/b è suddiviso in "canali". Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point vicini. L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "**Overlap**".
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1 posizionato sul canale 1, AP2 posizionato sul canale 6). Da questo si evince che soltanto 3 Access Point/Wireles Router possono essere usati in caso di sovrapposizioni spaziali (copertura) e temporali

(funzionamento contemporaneo).

Nella sezione **System-Status** è possibile controllare lo stato del link wireless.

Wireless Status	
Connection	UP
Channel	1
Signal Level	100%
TX Rate	54Mbps

PPPoE

In questa sezione è possibile effettuare la configurazione del client PPPoE integrato nell'apparato.

Ethernet | Wireless | PPPoE | DDNS

Configuration

☑ Enable PPPoE

User Name: Test1

Password: •••••••••

☑ Send Email when IP change

Save Reload

Status

IP Address:	0.0.0.0
Default Router:	0.0.0.0
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
Connection State:	Disabled

Refresh

Spuntare la voce Enable PPPoE ed inserire poi username e password. Spuntando la voce Send Email when IP Change il dispositivo provvederà all'invio automatico di una mail di notifica quando l'IP viene rinnovato. Cliccare su Save per rendere permanenti le nuove impostazioni e su Reload per effettuare un riaggiornamento della pagina.

Nella sezione Status è possibile controllare lo stato della connessione e l'indirizzo IP assegnato dal server PPPoE. Cliccare su Refresh per aggiornare le informazioni mostrate a video.

Il Client Dynamic DNS può funzionare correttamente (aggiornare il server Dynamic DNS) solo se utilizzato quando nella NetCamera NVW è attivato anche il client PPPoE (altrimenti non è possibile per la NetCamera NVW aggiornare coerentemente il server Dynamic DNS).

DDNS

Tramite questa funzionalità è possibile registrare un dominio ed associarlo ad un IP dinamico ed effettuare così la configurazione/gestione remota dell'apparato.

I passaggi da seguire sono i seguenti:

- Registrare il proprio dominio gratuitamente e istantaneamente su **www.dyndns.org**.
- Configurare il client sulla NetCamera NVW inserendo i campi appropriati (**Domain Name**, **Username** e **Password**)

Ethernet | Wireless | PPPoE | DDNS

Dynamic DNS

DDNS Server ○Disabled ⦿DynDNS ○PeanutHull

Hostname (Domain):

Username (Passport):

Password:

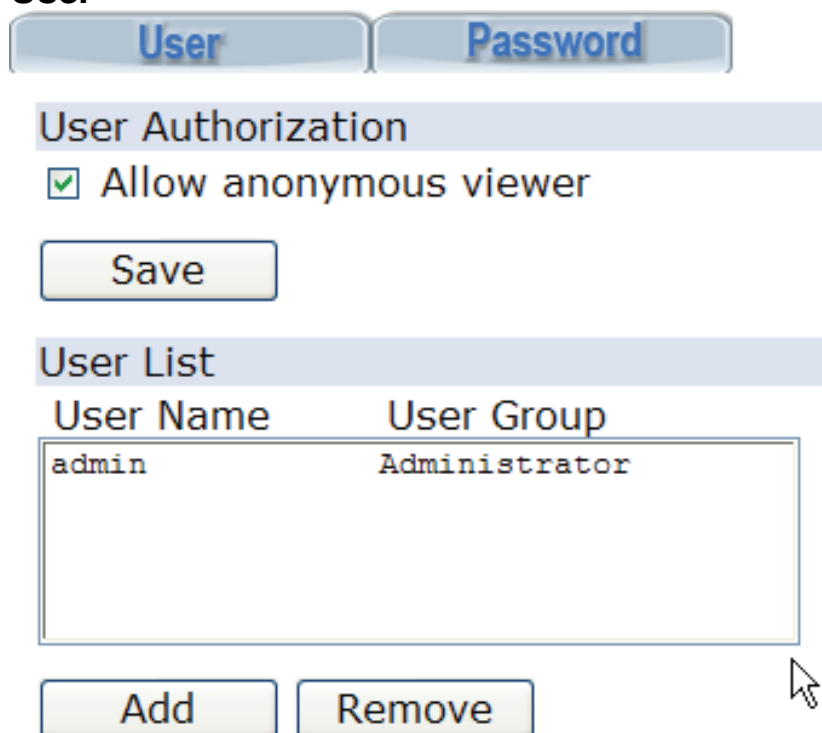
Status:

Save | Reload

A questo punto la NetCamera NVW è sempre e comunque raggiungibile dall'esterno.

Controllare la voce **Status** per controllare lo stato della registrazione presso il server Dynamic DNS.

Per ulteriori dettagli fare riferimento all'**Appendice A**.

Il Client Dynamic DNS può funzionare correttamente (aggiornare il server Dynamic DNS) solo se utilizzato quando nella NetCamera NVW è attivato anche il client PPPoE (altrimenti non è possibile per la NetCamera NVW aggiornare correttamente il server Dynamic DNS).

4.1.3 User

In questo sezione è possibile impostare le password di accesso all'apparato e definire differenti profili.

Una volta cliccato il menu **User** si apriranno le due seguenti sottosezioni:

- User
- Password

User

Nella sezione **User Authorization** è possibile permettere l'accesso alla home del dispositivo (non è possibile alcuna configurazione) senza che questo richieda alcuna password. Per fare questo spuntare la voce **Allow anonymous viewer** e cliccare su **Save.**

Nella sezione **User List** è invece possibile definire/rimuovere differenti utenti appartenenti a uno tra i 2 profili esistenti. Non è possibile rimuovere il profilo Administrator.

Cliccare su **Add,** introdurre username e password ed associare poi l'utente al profilo (User o Administrator). Cliccare poi su **Save**, il dispositivo visualizzerà nel campo **User List** il nuovo profilo.

Il profilo **User** permette solo l'accesso alla Home della NetCamera NVW mentre il profilo **Administrator** ne permette la piena configurazione.

Password
In questa sezione è possibile modificare la password di accesso del profilo. Introdurre la username e poi la nuova password di accesso (2 volte). Cliccare infine su **Save.**

4.1.4 Video

Una volta cliccato il menu **Video** si apriranno tutte le seguenti sottosezioni:

- Video
- Audio

Video

Nella sezione **Network Traffic Control** è possibile impostare il livello di bit-rate MPEG4 generato dalla NetCamera NVW. E' importante valutare la capacità massima dell'infrastruttura di rete al fine di evitare la saturazione di quest'ultima che porterebbe ad un decadimento delle prestazioni video.

Spuntare una delle seguenti voci:

- **High(>1.5Mbps):** Ideale per un uso in LAN/WLAN o in connessioni molto veloci
- **Medium(>0.5Mbps ma <1.5Mbpps**): Ideale per un uso in Wireless LAN con molte NetCamera NVW collegate
- **Low(<0.5Mbps):**Ideale per un controllo remoto video via ADSL
- **Resolution:** Impostare la risoluzione nella combo bar tra **VGA(640x480)** o **QVGA(320x240)**
- **Compression:**Impostare il livello di compressione uitilizzato nelle immagini. Più alto è il livello di compressione, minore sarà il bit rate utilizzato ma la qualità d'immagine sarà estremamente povera. Sono disponibili 5 livelli di comprensione.
- **Maximal Frame Rate:** Scegliere il livello di frame per secondo di video. Questo valore deve essere minore di 30fps.
- **P-Frame/I-Frame ratio**: Impostare il rapporto tra frame di tipo P/I. I frame sono di tipo differenziale (vengono immagazzinate le sole differenze rispetto ad un frame di riferimento) ed assolute (il frame è di fatto una JPG). Mettere 30 significa inviare un frame completo ogni 30 frame. Più basso è questo valore, migliore è il video (soprattutto se questo è un oggetto in rapido movimento), ma più alto è il bit-rate.

Video | Audio

Network Traffic Control (from camera to computer)

- ○ High (more than 1.5 Mbps, LAN, Inside House)
- ○ Medium (512 Kbps ~ 1.5 Mbps, LAN with many cameras)
- ⦿ Low (less than 512 Kbps, Internet, DSL, Cable)

Resolution: VGA 640x480

Compression: Medium (Higher compression, lower traffic.)

Maximal frame rate: 30 frames per second (1~30)

P-Frame / I-Frame Ratio: 30 (Higher ratio, lower traffic.)

Image Parameters [Default]

Brightness:	-	-1	+
Contrast:	-	2	+
Saturation:	-	0	+
Hue:	-	-1	+

- ☐ Vertical Flip
- ☐ Horizontal Flip
- ☑ Show Camera Name
- ☑ Show Time Label

IPCam-5C24 2006-11-17 12:54:39

Snapshot & Record

Snapshot Path c:\IPCam-5C24\ (must exist)

Record Path c:\IPCam-5C24\ (must exist)

Split recording file every 10 minutes

[Save] [Reload]

Nella sezione **Image Parameters** è possibile cambiare tutta una serie di parametri video:

- **Default**: cliccare sul bottone per riportare la sezione video alle impostazioni di default.
- **Brightness**: e' possibile impostare il livello di luminosità

- **Contrast**: e' possibile impostare il livello di contrasto
- **Saturation**: e' possibile impostare il livello di saturazione del colore
- **HUE**: e' possibile impostare il livello di tonalità colore
- **Vertical Flip**: effettua l'inversione verticale
- **Horizontal Flip**: effettua l'inversione orizzontale
- **Show Camera Name**: Mostra, sul video/picture, un campo contenente il parametro Camera Name (**System->Status**)
- **Show Time Label**: Mostra, sul video/picture, un campo contenente il parametro **Current Camera Time** contenente data e ora (**System->Time**)

Nella sezione **Snapshot & Record** è possibile impostare le path per il salvataggio dei video/snapshot. Inoltre, nel campo **Split record file every X minutes** è possibile introdurre un valore indicante ogni quanti minuti di registrazione deve durare un singolo file video. Cliccare su **Save** per rendere permanenti le nuove impostazioni o su **Reload** per ricaricare la videata attuale.

Nell'appendice D è contenuta una descrizione del funzionamento della compressione MPEG4.

Audio

In questa sezione è possibile attivare il microfono incorporato nella NetCamera NVW.

Spuntare **Enable Audio.**

Il sistema di compressione dell'audio ADPCM permette di ridurre il bit-rate utilizzato salvaguardandone l'intellegibilità. Sono disponibili 4 differenti impostazioni di compressione (in **Bit Rate**) che vanno da 16kbps sino a 40kbps. In **Audio Volume** è possibile selezionare il livello di registrazione del microfono.

Il sistema di campionamento **PCM** utilizza una quantizzazione con intervalli fissi (tra un minimo ed un massimo). Tutti i segnali in ingresso, compresi in un intervallo, producono lo stesso segnale campionato in uscita. Più piccolo è l'intervallo di quantizzazione, minore è l'errore introdotto ma più alto è il bit-rate.

Nell'**ADPCM** invece viene quantizzata la sola differenza tra il campione predetto e quello vero. Il risparmio di bit è importante.

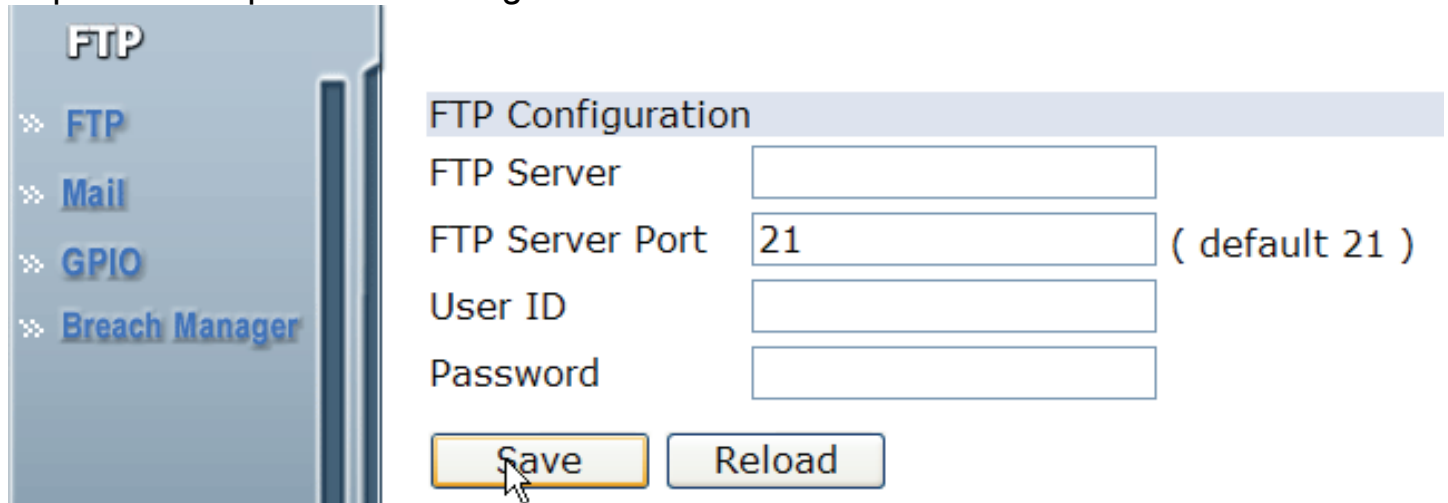
4.1.5 Video Player

Una volta cliccato il menu **Video Player** è possibile convertire i file generati dalla NetCamera NVW in video AVI (è necessario installare il codec DivX) o JPG.

Anzitutto cliccalre su **Sfoglia** ed indicare il percorso dove è contenuto il file con estensione AV. Premere **Play** per visualizzare il Video e **Stop** per interrompere.

Cliccare su **Transform Recording File to AVI Format** per convertire il video in formato AVI.

Cliccare su **Transform FTP File to JPEG Format** per convertire le immagini salvate in formato JPEG (spuantare la voce **Transform all files in the same folder** per far salvare TUTTI i file con estensione jpg nello stesso percorso dei files iniziali).

Non utilizzare queste funzionalità se il Motion Detection è attivo.

4.2 Advanced

In questa sezione della NetCamera NVW è possibile impostare il server FTP remoto, l'indirizzo mail cui spedire le varie notifiche, la avanzate funzioni di commutazione (2x DI in ingresso, 1x DO in uscita ed infine l'impostazione del motion detection.

4.2.1 FTP

E' possibile impostare la configurazione del server FTP remoto.

Introdurre l'indirizzo IP del server FTP, la porta utilizzata (generalmente la 21), la user ID e la password.

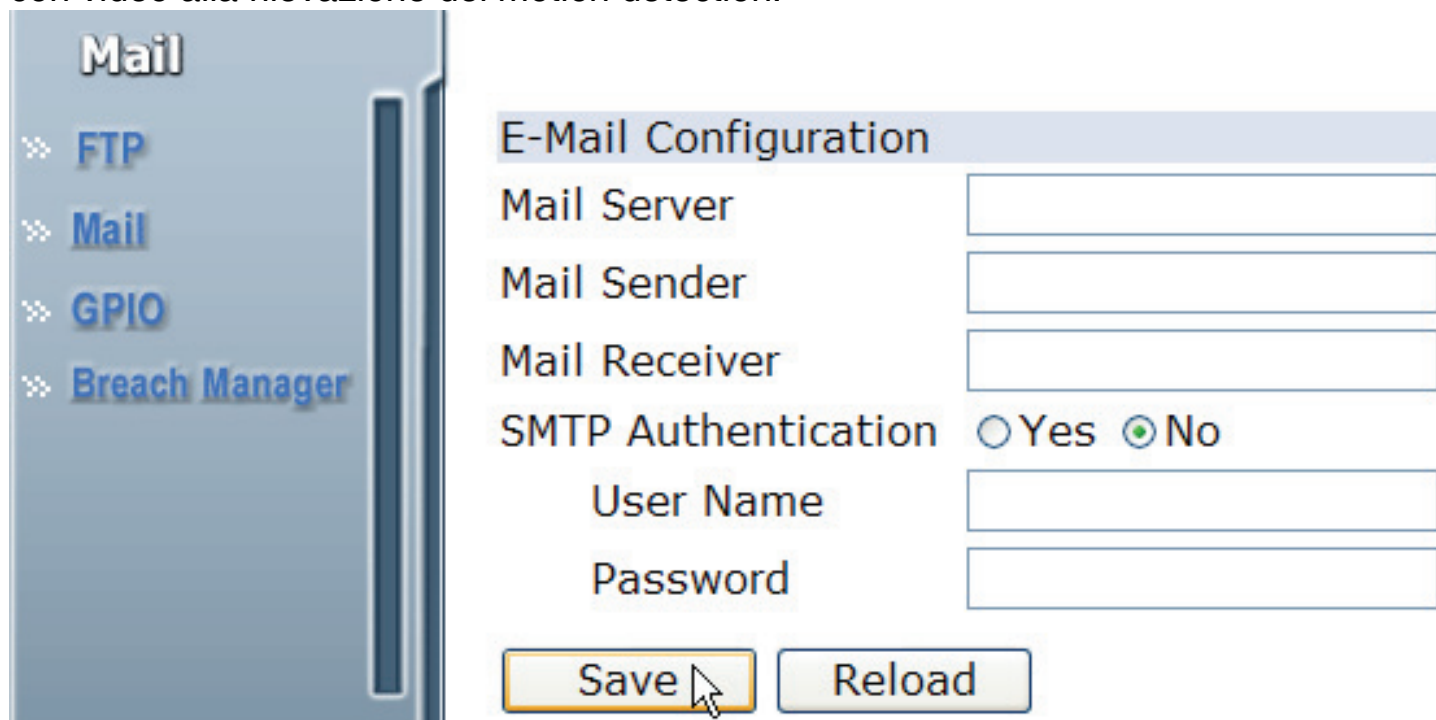
Quando il server FTP viene abilitato, la NetCamera NVW invierà le immagini sul server impostato (verificare che sia attiva tale funzionalità nel MENU **Breach Manager**).

Motion Detection

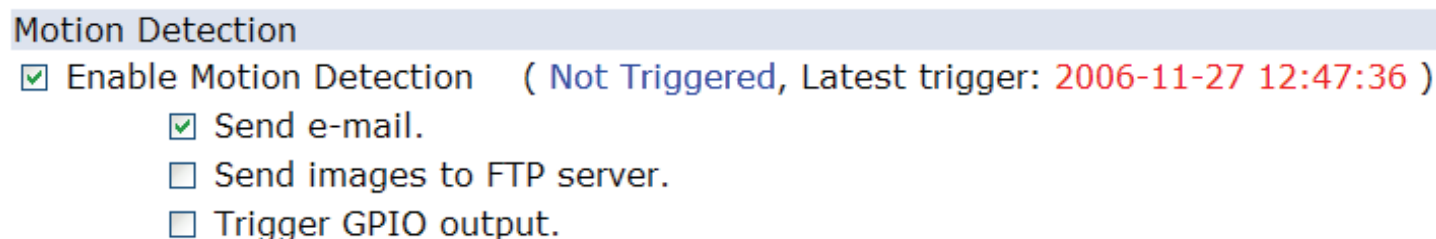
☑ Enable Motion Detection (Not Triggered, Latest trigger: 2006-11-27 12:47:36)

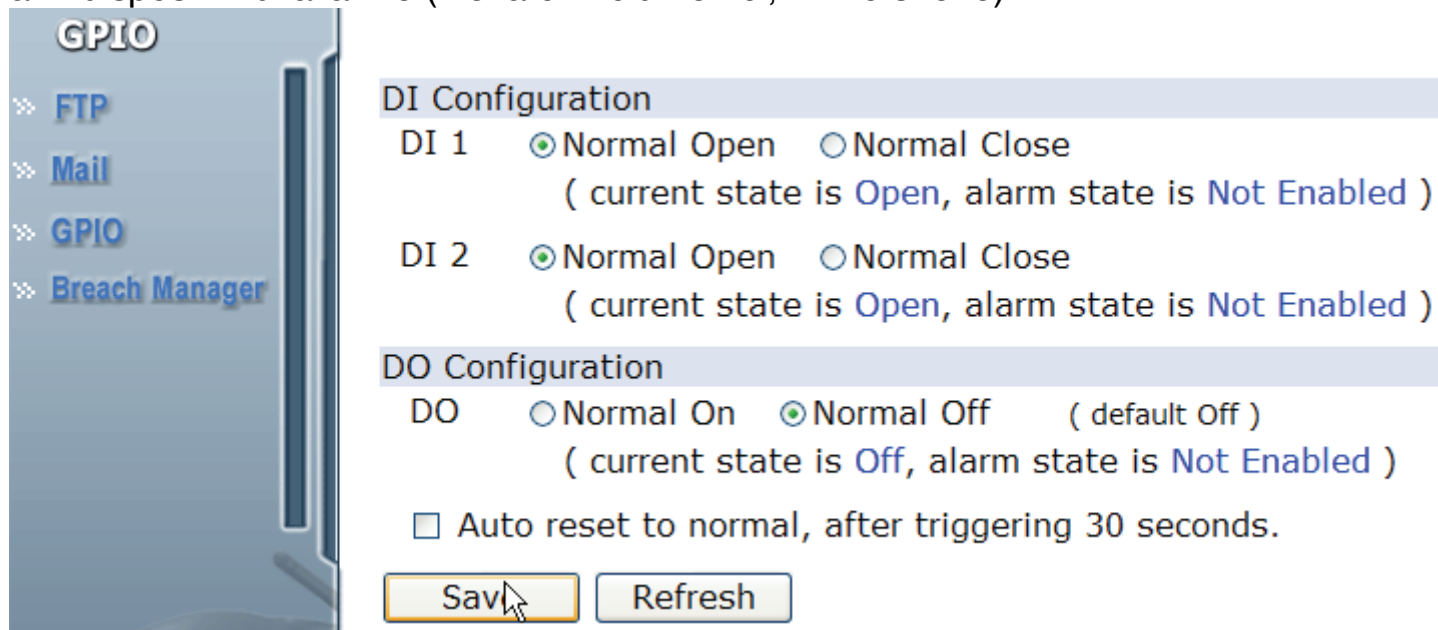
☐ Send e-mail.

☑ Send images to FTP server.

☐ Trigger GPIO output.

Cliccare infine su **Save** per rendere permanente la configurazione.

I File salvati sul server FTP sono con estensione AV. Consulare la sezione 4.1.5 per effettuarne la conversione in JPG.

4.2.2 Mail

E' possibile impostare la configurazione del server SMTP e inviare partanto una mail con video alla rilevazione del motion detection.

Introdurre l'indirizzo IP o nome del mail server, l'indirizzo mail del ricevente e l'indirizzo del mittente.
Nell'ipotesi in cui il server SMTP necessiti di autenticazione spuntare la voce SMTP Authentication (selezionare Yes) ed introdurre poi username e password.

Quando la configurazione **E-Mail Configuration** viene abilitata, la NetCamera NVW invierà il video all'indirizzo di mail impostato (verificare che sia attiva tale funzionalità nel MENU **Breach Manager**).

Motion Detection

☑ Enable Motion Detection (Not Triggered, Latest trigger: 2006-11-27 12:47:36)

☑ Send e-mail.
☐ Send images to FTP server.
☐ Trigger GPIO output.

Cliccare infine su **Save** per rendere permanente la configurazione.

4.2.3 GPIO

E’ possibile impostare la configurazione avanzate delle funzioni di commutazione (2x DI in ingresso, 1x DO in uscita) che rendono possibili la ricezione/invio di segnali ad altri dispositivi di allarme (rilevatori volumetrici, PIR o sirene).

E’ possibile collegare al retro della telecamere (nelle apposite porte) un sensore opportuno. Sono presenti 2 porte **DI** che possono essere configurate come normalmente aperte o chiuse. Un sensore impostato come “normalmente aperto” è come un interruttore aperto che viene chiuso se pilotato da un evento (triggered). Un sensore impostato come “normalmente chiuso” è come un interruttore acceso che viene aperto se pilotato da un evento (triggered).

Gli ingressi DI devono essere collegati a dispositivi esterni opportuni per funzionare correttamente.

La porta **DO** invece può essere utilizzate per pilotare un dispositivo esterno. Valgono le stesse considerazione prime espresse per i **DI**. Cliccare infine su **Save** per rendere permanente la configurazione.

Spuntando la voce **Auto reset to normal, after triggering 30 seconds**, dopo 30 secondi l’interruttore torna nello stato non triggered. Se nel frattempo vi è un altro evento che genera un trigger il contatore viene azzerato. E’ opportuno notare che durante tutto questo tempo, se attivato l’upload su FTP, diverse immagini

verranno caricate.

4.2.4 Breach Manager

In questa sezione è possibile:

- abilitare il motion detection e prevedere l'invio di Mail/FTP/DO
- controllare tramite i 2 DI tutta una serie di eventi quali Mail/FTP/DO o abilitare la rilevazione del movimento

Motion Detection

☑ Enable Motion Detection (Not Triggered, Latest trigger: 2006-11-27 12:56:55)
- ☐ Send e-mail.
- ☑ Send images to FTP server.
- ☐ Trigger GPIO output.

GPIO DI

☐ Enable DI 1 (Not Enabled, Latest trigger:)
- ☐ Send e-mail.
- ☐ Send images to FTP server.
- ☐ Trigger GPIO output.
- ☐ Enable motion detection, if it is not enabled.

☐ Enable DI 2 (Not Enabled, Latest trigger:)
- ☐ Send e-mail.
- ☐ Send images to FTP server.
- ☐ Trigger GPIO output.
- ☐ Enable motion detection, if it is not enabled.

[Save] [Refresh] [Clear Alarm]

Nella sezione **Motion Detection** (una volta spuntata) è possibile attivare l'invio di Mail, l'upload di immagini sul server FTP o cambiare lo stato del DO.

Nella sezione **GPIO DI** invece è possibile attivare, per ognuno dei 2 DI, l'invio Mail, l'upload di immagini sul server FTP, cambiare lo stato del DO o attivare il Motion Detection (se non già attivato).

Attivando un DI in ingresso è possibile configurare il sistema affinché invii mail o faccia l'upload di immagini su un server FTP remoto.

Tramite il DO è possibile pilotare un allarme esterno, quale ad esempio una sirena. Una volta attivato il Motion Detection o DI infatti è possibile cambiare stato al DO (enable Trigger GPIO output).

Capitolo 5

Supporto Offerto

5.1 Supporto Offerto

Per ogni problema con questo dispositivo consultare il manuale completo fornito a corredo sul CDRom.
Per qualunque altro problema o dubbio (prima è opportuno munirsi del seriale e codice prodotto) è possibile contattare l'help desk telefonico (**02/93907634**) gratuito di Atlantis Land che fornirà assistenza da lunedì al giovedì dalle 9:00 alle 13:00 e dalle 14:00 alle 18:00 ed il venerdì dalle 9:00 alle 13:00. E' possibile anche utilizzare il fax (02/93906161) la posta elettronica (info@atlantis-land.com oppure tecnici@atlantis-land.com) per esporre eventuali domande o problemi.

Atlantis Land SpA
Viale De Gasperi 122
20017 Mazzo di Rho (MI)

Tel: +39.(0)2.93906085 (Fax: +39.(0)2.93906161)
Help Desk :+39.(0)2.93907634

APPENDICE A: Risoluzione dei problemi

Questo capitolo illustra come identificare e risolvere eventuali problemi sulla NetCamera NVW.

A.1 LEDs

I LEDs sono un utile strumento per individuare eventuali problemi, osservandone lo stato è possibile individuare velocemente dove si verifica un eventuale malfunzionamento.

A.1.1 LED Power

Il LED PWR non si accende

Steps	Azione Correttiva
1	Accertarsi che l'alimentatore sia connesso alla NetCamera NVW ed alla rete elettrica. Utilizzare unicamente l'alimentatore fornito a corredo.
2	Verificare che l'alimentatore sia connesso ad una presa elettrica attiva e in grado di fornire la tensione necessaria al funzionamento del prodotto.
3	Accertarsi che il Plug dell'alimentatore sia correttamente inserito.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

A.1.2 LED LAN

Il LED LAN non si accende.

Steps	Azione Correttiva
1	Verificare la connessione del cavo di rete tra la NetCamera NVW e il PC o lo Switch di rete.
2	Verificare che il cavo sia funzionante.
3	Verificare che la scheda di rete del PC funzioni correttamente.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

A.2 Configurazione WEB

Non è possible accedere all'interfaccia Web di configurazione.

Steps	Azione correttiva
1	Accertarsi di utilizzare un indirizzo IP corretto, appartenente alla stessa rete della NetCamera NVW (192.168.1.x).
3	Provare ad effettuare un ping verso l'IP della NetCamera NVW.
4	Effettuare un reset del dispositivo.

Le schermate di configurazione Web non vengono visualizzate correttamente.

Steps	Azione correttiva
1	Accertarsi di utilizzare Internet Explorer 5 o una versione successiva.
2	Installare ActiveX.
3	Eliminare i files temporanei di Internet ed eseguire un nuovo login.

A.3 Login con Username e Password

E' stata dimenticata la password di accesso.

Steps	Azione correttiva
1	Se è stata cambiata la password di accesso ed è stata dimenticata, sarà necessario caricare la configurazione di default. Ciò cancellerà tutte le configurazioni eseguite dall'utente e ripristinerà la password di default. Premendo il pulsante **Reset** presente nel pannello anteriore per una decina secondi, la NetCamera NVW riporterà tutte le impostazioni ai valori iniziali.
2	I parametri di default per l'accesso alla configurazione della NetCamera NVW sono: **Username: admin** **Password: admin** **IP:192.168.1.1**
3	Per incrementare il livello di sicurezza del sistema è molto importante modificare la password di default.

A.4 Amministrazione remota

Non è possibile amministrare la NetCamera NVW da remoto.

Steps	Azione correttiva
1	Assicurarsi di aver messo l'IP del Router ADSL (il cui IP pubblico viene usato per la configurazione remota) nal campo default Gateway della NetCamera NVW.
2	Assicurarsi che nel Router ADSL siano corretti i settaggi (creare un Virtual Server dalla porta 80 all'IP privato della NetCamera NVW)

A.5 Domande Generali

Domanda	Cos'è una IP Wireless Security Night Vision Camera?
Risposta	Il dispositivo è un apparato indipendente, dotato di una propria CPU, che va collegato direttamente alla LAN (tramite cavo o via wireless). NetCamera NVW può essere gestita e controllata anche da remoto, in maniera semplice ed intuitiva, tramite un PC o portatile collegato in Internet (o Intranet) utilizzando un qualsiasi browser web (con Active X) in qualunque momento e luogo.

Domanda	Quanti utenti contemporaneamente possono accedere al dispositivo?
Risposta	Il numero massimo di utenti permesso è 20. E' opportuno considerare che questo è il numero massimo teorico e che le performance offerte potrebbero decadere drasticamente.

Domanda	Che algoritmo viene utilizzato per la compressione delle immagini?
Risposta	Il dispositivo utilizza lo standard MPEG4 offrendo contemporaneamente una bassa occupazione in banda ed una buona qualità video. Si faccia riferimento, per approfondimenti, all'opportuna Appendice.

Domanda	A che distanza posso utilizzare l'IP Wireless Security Nigh Vision Camera?

Risposta	La distanza massima teorica dipende da moltissimi fattori e può arrivare sino a 100m in ambienti indoor e sino a 300m in ambienti outdoor. E' bene tenere a mente che questi sono davvero i valori massimi ottenibili in condizioni assolutamente ideali. Numerosi fattori possono drasticamente diminuire la copertura (ad esempio: apparati RF, rumore, muri, strutture metalliche etc). L'esperienza pratica consiglia di considerare in indoor 30m ed in outdoor 80m. Si faccia riferimento, per approfondimenti, all'opportuna Appendice.

Domanda	**E' possible utilizzare l'IP Wireless Security Night Vision Camera in ambienti esterni?**
Risposta	No, il dispositivo non va assolutamente utilizzato in ambienti esterni.

Domanda	**Che tipo di cavo va utilizzato per collegare l'IP Wireless Security Night Vision Camera alla rete LAN?**
Risposta	Utilizzare un cavo Cat 5 UTP (presente anche nella scatola).

Domanda	**E' possible utilizzare l'IP Wireless Security Night Vision Camera come una WEB Cam?**
Risposta	No, il dispositivo è basato sul protocollo IP è può essere collegata al PC solo attraverso il cavo di rete (o via Wireless) e non viene da quest'ultimo riconosciuta come una periferica di acquisizione video.

Domanda	**E' possible collegare l' IP Wireless Security Night Vision Camera ad una rete di IP privati?**
Rispsosta	Certo, anzi questo è il caso di utilizzo più commune. In questo caso è però opportuno valutare i seguenti accorgimenti al fine di poter realizzare un controllo remoto del dispositivo:

	1) Configurare correttamente l'IP gateway della NetCamera (come Default Gateway va messo l'IP lato LAN del Router ADSL) 2) Nella sezione del Virtual Server del router ADSL ruotare la porta 80 (o quella scelta per il controllo del dispositivo) sull'IP della NetCamera 3) Disabilitare eventuali Firewall o aprire la porta usata dalla NetCamera (solitamente la 80) A questo punto, da remoto, digitando l'IP (se questo non è dotato di IP fisso, leggere la sezione Dynamic DNS) del Router ADSL è possibile controllare NetCamera come se si fosse nella LAN locale.

Domanda	**E' possibile installare ed utilizzare una IP Wireless Security Night Vision Camera dietro un firewall?**
Risposta	Si, è sufficiente aprire sul firewall la porta 80 (o la porta su cui si è deciso di impostare il dispositivo).

Domanda	**Cos'è lo Spread Spectrum?**
Risposta	La trasmissione Spread Spectrum si basa sulla dispersione dell'informazione su una banda molto più ampia di quella necessaria alla modulazione del segnale disponibile. Il vantaggio che si ottiene da questa tecnica di modulazione è infatti una bassa sensibilità ai disturbi radioelettrici anche per trasmissioni a potenza limitata. Questa caratteristica è ovviamente preziosa quando si devono trasmettere dei dati.

Domanda	**Cosa sono DSSS e FHHS?**
Risposta	DSSS (Direct-Sequence Spread-Spectrum): E' una particolare tecnologia di trasmissione per la banda larga che consente di trasmettere ogni bit in maniera ridondante. E' adatta in particolare per la trasmissione e la ricezione di segnali deboli. FHHS (Frequency Hopping Spread Spectrum): è una

	tecnologia che permette la condivisione tra più utenti di uno stesso insieme di frequenze. Per evitare interferenze tra periferiche dello stesso tipo le frequenze di trasmissione cambiano sino a 1.600 volte ogni secondo.

Domanda	**Le informazioni inviate via wireless possono essere intercettate?**
Risposta	La NetCamera NVW offre funzionalità di crittografia WEP fino a 128 bit, ciò provvede a rendere sicure le trasmissioni dati wireless. L'utilizzo del WPA rende ancora più sicura la trasmissione wireless.

Domanda	**Cosa è il WEP?**
Risposta	Il segnale radio, come già evidenziato in precedenza, è di difficile contenimento è può pertanto essere intercettato da utenti non autorizzati (è sufficiente che abbiano un comune client wireless in standard IEEE802.11b/g). Il protocollo WEP nasce per limitare questo fenomeno. WEP è la sigla di Wired Equivalent Privacy, un protocollo di sicurezza per le reti locali senza fili (WLAN) definito dallo standard 802.11b. Nel dettaglio i servizi offerti dal WEP sono: • autenticazione delle stazioni che accedono ai servizi di rete • integrità dei dati trasmessi sul canale radio (nessuna cambiamento è possibile senza che il sistema non se ne accorga) • riservatezza dei dati trasmessi sul canale radio (nessuno può comprendere l'informazione contenuta nei pacchetti che sono cifrati con l'algoritmo RC4)

Domanda	**Cosa è il WPA?**
Risposta	In attesa delle ratifica dello standard IEEE802.11i la Wi-Fi Alliance ha derivato dalla versione preliminare un insieme di specifiche che va sotto il nome di WPA (Wi-Fi Protected

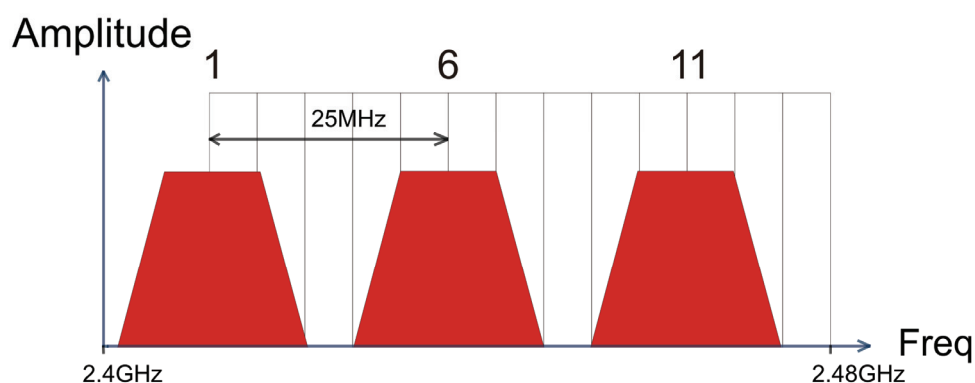
	Access). Le caratteristiche peculiari del WPA sono: • Integrazione del TKIP (Temporal Key Integrity Protocol) per permettere il cambio della chiave e migliora il controllo di integrità dei pacchetti • Meccanismo avanzato per gestire l'autenticazione e il controllo degli accessi ai servizi di rete in modo centralizzato (802.11x tramite EAP, l'uso di TLS è obbligatorio) • La chiave di autenticazione è diversa da quella utilizzata per la cifratura (che grazie al TKIP cambia continuamente) • Permette l'autenticazione direttamente sull'AP (WPA-PSK) Tale protocollo è molto più robusto del WEP.

Domanda	**Cosa è il WPA2?**
Risposta	Approvato di recente dalla Wi-Fi Alliance, il nuovo standard WPA2 è l'evoluzione del primo WPA (Wi-Fi Protected Access) che è oggi supportato dalla maggior parte degli apparati compatibili IEEE802.11g. Lo standard WPA, richiesto prepotentemente dal mercato per porre fine alla debolezza intrinseca del WEP, ha purtroppo tratto dall'802.11i solo una parte delle specifiche. Il nuovo WPA2 invece abbracciando pienamente l'IEEE802.11i ha necessariamente introdotto il supporto per l'Advanced Encryption Standard (AES), protocollo di cifrature utilizzato già da tempo nelle VPN IPSec. I dispositivi WPA2 saranno compatibili con quelli WPA che però dovranno essere riaggiornati tramite il rilascio di nuovi firmware e/o driver. Il problema risiede nella capacità di calcolo (richiesta dall'AES) che rischierebbe di essere praticamente troppo elevata per gli apparati oggi in commercio.

Domanda	Cosa è la modalità Infrastructure?
Risposta	Nella configurazione Infrastructure una rete WLAN e una rete WAN comunicano tra loro tramite un access point.

Domanda	Cosa è la banda ISM?
Risposta	Questa frequenza è stata messa a disposizione dalla FCC, su richiesta delle aziende che intendevano sviluppare soluzioni wireless per l'uso civile quotidiano ed è generalmente contraddistinta dalla sigla ISM band (Industrial, Scientific and Medical). In questa frequenza operano solo dispositivi industriali, scientifici e medici a basse potenze.

Domanda	Cosa è lo standard IEEE 802.11g ?
Risposta	Il nuovo standard 802.11g opera alla frequenza di 2,4 GHz e quindi è pienamente compatibile con la più diffusa versione b. Il vantaggio è che consente una velocità di trasferimento di 54 Mbps, cinque volte superiore allo standard 802.11b.

Domanda	Perché 2 AP benché utilizzino differenti canali interferiscono tra di loro?
Risposta	Ogni canale occupa all'incirca 22Mhz, essendo l'intera banda ISM di 80Mhz possono essere utilizzati contemporaneamente soltanto 3 dei 13 canali disponibili. E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6). L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap". Il disegno seguente illustra meglio quanto detto:

	Sino a 3 AP possono coesistere senza overlapping. E' opportuno prestare attenzione all'assegnazione dei canali.

Domanda	**I client IEEE802.11b funzionano con AP IEEE802.11g?**
Risposta	Senza alcun dubbio è possibile utilizzare client IEEE802.11b con AP IEEE802.11g. In questo caso si crea una WLAN ibrida. Le prestazioni ottenibili dai client IEEE802.11g risultano essere di gran lunga peggiori in una rete ibrida che non in una WLAN con solo apparati IEEE802.11g. Il consiglio è quello di migrare l'intera WLAN verso client IEEE802.11g.

Domanda	**Come posso eliminare le interferenze che deteriorano le prestazioni della WLAN?**
Risposta	Anzitutto spegnere (o allontanare) ogni dispositivo che operi nelle stesse frequenze. Utilizzare antenne direzionali per far "imbarcare" meno rumore ai dispositivi. In caso si altri AP adiacenti consultare la faq sull'assegnazione dei canali.

Domanda	**Introduzione ai decibel (cos'è)?**
Risposta	Il deciBel è un'unita misura relativa che esprime un rapporto fra 2 valori. E' importante sottolineare che è adimensionale (non si misura in watt) e permette di capire immediatamente lo scostamento dalla misura campione o riferimento. E' utilizzato

	perché permette di avere un'immediata percezione della differenza di 2 misurazioni, essendo il logaritmo una misura compressa e non lineare. L'equazione canonica è la seguente: dB = 10 log10 (P 2 / P 1). Dove P1 è la misura riferimento e P 2 è la misura istantanea.

Domanda	**Introduzione al dBm (cos'è)?**
Risposta	Definiamo il dBm=10 log 10 (P 2 / P 1), dove P1 =1 milliWatt (mW). E' possibile pertanto parlare di potenza trasmessa sia utilizzando il watt che il dBm. Nella tabella seguente è riportata l'equivalenza per i valori più comuni (utilizzare la formula di sopra per valori non in tabella):

dBm	**Watt**	**note**
0	1 mW	
3	2 mW	
6	4 mW	
9	8 mW	
10	10 mW	
12	15,8 mW	
13	20 mW	
14	25 mW	
15	32 mW	
16	40 mW	
17	50 mW	
18	63 mW	
19	79 mW	
20	100 mW	Massima Potenza utilizzabil 2.4Ghz
23	200 mW	
26	400 mW	
29	800 mW	

Domanda	Cos’ è un’antenna Isotropica?
Risposta	Antenna che irraggia senza prediligere alcuna specifica direzione nello spazio circostante. E’ possibile fare un paragone con l’irraggiamento luminoso di una lampadina che avviene uniformemente in tutto lo spazio circostante. Effettuando una rilevazione della densità superficiale di potenza su una superficie sferica, il cui centro è posto sull’antenna, questa è uniforme. Tale valore, espresso in [W]/[m^2], è legato all’inverso del quadrato della distanza tra il punto in cui si effettua la rilevazione e la sorgente (punto da cui l’antenna irraggia il segnale). L’antenna integrata nella NetCamera NVW è di tipo isotropico.

Domanda	Cos’ è un’antenna Direttiva(con un certo guadagno)?
Risposta	Il guadagno di un'antenna è definito come il rapporto fra la potenza irradiata dall'antenna in esame nella direzione di massima direttività e la potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza.

Domanda	Cos’ è il dBi?
Risposta	Il guadagno di un'antenna è definito come il rapporto fra la densità di potenza irradiata dall'antenna in esame nella direzione di massima direttività (P 2) e la densità di potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza. Definiamo il dBi=10 log 10 (P 2 / P isotropica), dBm=10 log 10 (Potenza/ 1mW)

APPENDICE B: Trouble Shooting

In questo capitolo vengono evidenziati tutta una serie di problematiche e le relative soluzione.

Domanda	Il dispositivo non è raggiungibile per la configurazione WEB.
Risposta	La causa potrebbe essere una sovrapposizione di indirizzi IP. Staccare NetCamera NVW dalla LAN e ricollegarla direttamente al PC ed eseguire il commando PING. Lanciare una finestra DOS: Scrivere **ping 192.168.1.1** e cliccare su enter. Se la telecamera risponde allora l'ipotesi della sovrapposizione di indirizzi IP è verificata, in caso contrario controllare l'indirizzo IP del proprio PC verificando che sia nella stessa classe della NetCamera NVW (192.168.1.x con x compreso tra 2 e 254). Se una volta verificata anche la correttezza della classe di appartenenze del PC, la NetCamera NVW non rispondesse provare ad effettuare il reset. Se anche dopo il reset il dispositivo non dovesse rispondere contattare l'assistenza tecnica.

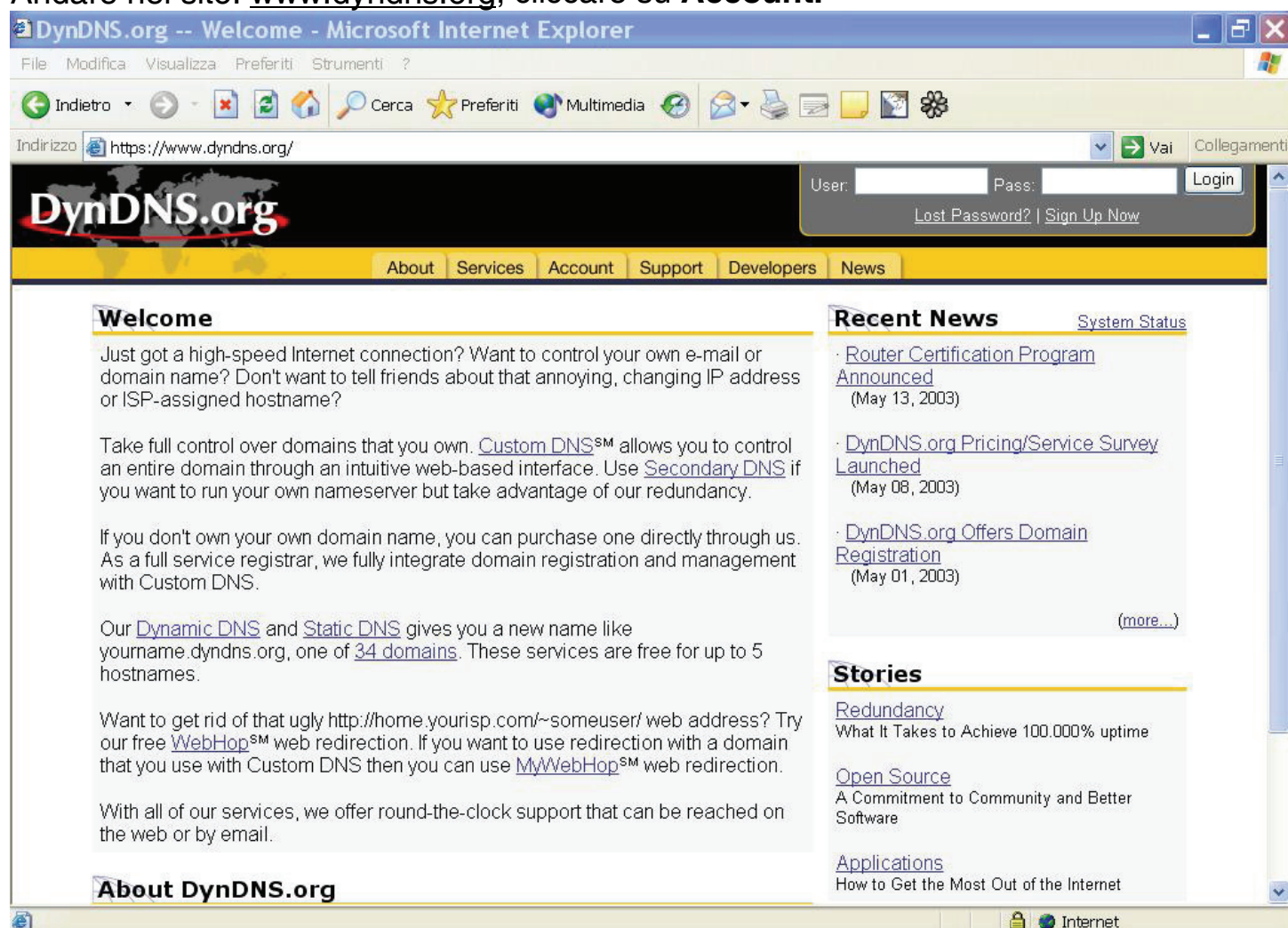
Domanda	Perché il LED Power non è acceso continuamente?
Risposta	Verificare che l'alimentatore sia quello fornito a corredo (DC 5V) e che sia saldamente inserito nella presa a muro.

Domanda	L'accesso remoto alla NetCamera NVW non funziona!
Risposta	• Verificare eventuali Firewall ed aprire la porta 80 • Verificare che il default Gatewy della NetCamera NVW sia l'IP lato LAN del Router ADSL. • Effettuare una rotazione della porta 80 nella sezione Virtual Server del Router ADSL verso l'IP della NetCamera NVW • Controllare che l'IP del Router ADSL sia corretto.

Domanda	L'immagine è sfocata. Come è possible migliorare la messa a fuoco dell'apparato?
Risposta	La NetCamera NVW ha una messa a fuoco manuale. Ruotare delicatamente la ghiera sino ad ottenere la messa a fuoco più adatta. Ulteriori dettagli sono contenuti nell'Appendice opportuna.

Domanda	La qualità video è deludente, come è possible migliorarla?
Risposta	• Controllare il numero di colori a video e forzare il video ad almeno 16 bit colore. • E' possible calibrare i parametri video nella sezione Advanced/Video.

Domanda	Nel browser non sono visualizzate immagini!
Risposta	Attivare il controllo Active X. Verificare che il browser utilizzato supporti Active X.

Domanda	E’ possible catturare immagini dalla NetCamera NVW?
Risposta	Si, è possible slavare l’immagine a video direttamente come imagine. Fare riferimento alla sezione 3.3.

APPENDICE C: Dynamic DNS

Grazie all'adozione di questa features è possibile registrare un dominio pur se associato ad un IP dinamico. Ci sono una moltitudine di server DDNS che offrono gratuitamente questo tipo di servizio. E' sufficiente registrarsi per attivare in maniera gratuita ed immediata il servizio che consentirà di raggiungere (da remoto) sempre la NetCamera NVW.

Ogni qual volta la NetCamera NVW si riconnetterà, tramite il client incorporato, comunicherà al server DDNS il nuovo indirizzo IP. In questo modo chiunque dall'esterno conoscendo l'URL conoscerà anche l'indirizzo IP che in quel momento è stato assegnato alla NetCamera NVW.

Vediamo, nel dettaglio come effettuare una registrazione con il gestore DDNS forse più famoso.

Andare nel sito: www.dyndns.org, cliccare su **Account.**

DynDNS.org -- Welcome - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indietro Cerca Preferiti Multimedia

Indirizzo https://www.dyndns.org/ Vai Collegamenti

DynDNS.org

User: Pass: Login

Lost Password? | Sign Up Now

About | Services | Account | Support | Developers | News

Welcome

Just got a high-speed Internet connection? Want to control your own e-mail or domain name? Don't want to tell friends about that annoying, changing IP address or ISP-assigned hostname?

Take full control over domains that you own. Custom DNS℠ allows you to control an entire domain through an intuitive web-based interface. Use Secondary DNS if you want to run your own nameserver but take advantage of our redundancy.

If you don't own your own domain name, you can purchase one directly through us. As a full service registrar, we fully integrate domain registration and management with Custom DNS.

Our Dynamic DNS and Static DNS gives you a new name like yourname.dyndns.org, one of 34 domains. These services are free for up to 5 hostnames.

Want to get rid of that ugly http://home.yourisp.com/~someuser/ web address? Try our free WebHop℠ web redirection. If you want to use redirection with a domain that you use with Custom DNS then you can use MyWebHop℠ web redirection.

With all of our services, we offer round-the-clock support that can be reached on the web or by email.

About DynDNS.org

Recent News System Status

· Router Certification Program Announced (May 13, 2003)

· DynDNS.org Pricing/Service Survey Launched (May 08, 2003)

· DynDNS.org Offers Domain Registration (May 01, 2003)

(more...)

Stories

Redundancy
What It Takes to Achieve 100.000% uptime

Open Source
A Commitment to Community and Better Software

Applications
How to Get the Most Out of the Internet

Internet

Effettuare la registrazione (cliccando su **Create Account**) inserendo: **Username, Indirizzo Mail e Password.**
Una mail di verifica registrazione sarà inviata all'indirizzo inserito. In questa mail sono contenute le istruzioni per proseguire la registrazione (è necessario confermare così il tutto entro 48 ore). Seguire le istruzioni contenute e compilare il form per terminare la fase di registrazione.
A questo punto tornare nel sito, andare su **Services**, evidenziare (nella parte sinistra) il menù **Dynamic DNS** e poi cliccare su **Add Host**.
Non resta che introdurre il **Nome dell'host** (evidenziare Enable WildCard) e scegliere il suffisso preferito e premere poi sul bottone **Add Host** per terminare.

Passiamo adesso alla configurazione del client nella NetCamera NVW (nella sezione **Basic->Network->DDNS**).

Spuntare il bottone **DYnDNS**
Compilare il campo **Domain Name** inserendo per esteso il dominio registrato e inserire poi **Username** e **Password**.
Premere su **Save** per rendere permanenti le modifiche.
Andando sul sito www.dyndns.org, (effettuare il LogIn ed andare nella sezione Account poi sotto Dynamic DNS all'URL) è possibile controllare che l'IP sia stato aggiornato (alternativamente è possibile effettuare un ping verso il vostro URL).

APPENDICE D: MPEG4

Le IP Camera forniscono un flusso video continuo a 25 o 30 fps. Immaginiamo di utilizzare una risoluzione di 640*480 con 30 fps. Ogni immagine può occupare sino a (640*480*3 pixel, per ciascuno utilizziamo 1 Byte) 1 MByte (in BMP) e dunque un flusso video sino a 30MB/s Questo flusso video può arrivare ad occupare un'ampiezza di banda importante e può arrivare generare le seguenti problematiche:

Tipo di Rete	**Risultato**
LAN	Alto traffico
WLAN	Saturazione
ADSL	N/A

L'utilizzo della compressione JPEG, porta ad un risparmio importante di banda. Il video in questo caso arriva ad essere un flusso di immagini JPEG (tali video viene definito MJPEG). Come si vede a seconda della tipologia di compressione questi video possono passare da 1MB/s sino ad 2,5MB/s.

Tipo di Rete	**Risultato(Jpeg Low=24KB image)**	**Risultato(Jpeg Medium=40 KB image)**	**Risultato(Jpeg High =80 KB image)**
LAN	Ottimale	Ottimale	Ottimale
WLAN	Alto traffico	Alto traffico	Saturazione
ADSL	N/A	N/A	N/A

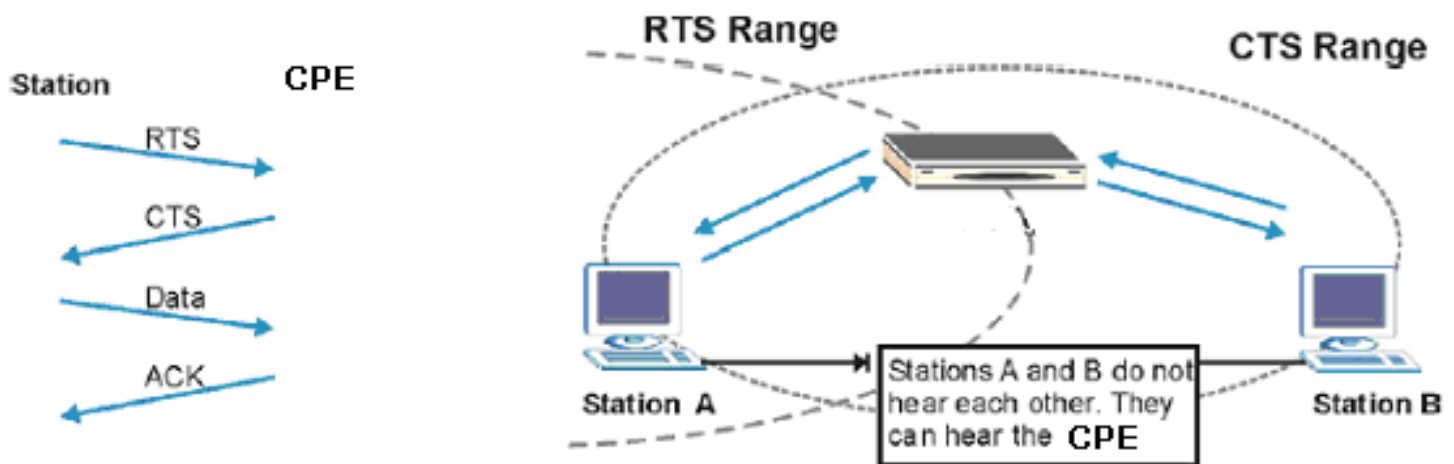
La compressione MPEG4 invece crea un flusso video che può variare da 500Kb/s sino a 1,5Mb/s risultando di gran lunga inferiore di quello di un video MJPEG.

Tipo di Rete	**Risultato(Low Quality 500Kb/s)**	**Risultato(Medium Quality = 1Mb/s)**	**Risultato(High Quality = 1Mb/s)**
LAN	Ottimale	Ottimale	Ottimale
WLAN	Ottimale	Ottimale	Ottimale
ADSL	Alto Traffico	Saturazione	N/A

Come si evince dalla tabella la compressione MPEG4 permette davvero di fruire di un video fluido in una rete LAN/WLAN, senza arrivare alla saturazione, ed utilizzare anche da remoto il dispositivo.

APPENDICE E: Come Avviene la comunicazione Wireless

La comunicazione in una WLAN avviene tramite onde radio che hanno una frequenza compresa tra 2.4Ghz e 2.48Ghz. Vengono dunque utilizzati circa 80Mhz di banda ISM (è una banda libera per applicazioni industriali, scientifiche e mediche).
La trasmissione avviene dunque utilizzando un mezzo condiviso e possono pertanto sorgere delle collisioni durante l'accesso da parte dei client wireless.
Il protocollo CSMA/CA ("carrier sense multiple access with collision avoidance") è responsabile di garantire una politica di accesso corretta al mezzo, limitando al massimo il numero di collisioni.
Un client(o nodo), infatti, prima di inviare un pacchetto dati si mette in ascolto e, rilevato il canale libero, invia i dati.

RTS/CTS
Quando due stazioni Wireless sono all'interno del range dello stesso Access Point ma non si vedono direttamente si ha un "nodo nascosto". La figura che segue illustra questa situazione.

La stazione A invia dei dati all'AP ma nel mentre non sa se la stazione B sta già utilizzando il canale. Se le due stazioni trasmettessero richieste di inizio trasmissione allo stesso tempo si avrebbero delle collisioni quando le informazioni giungono all'Access Point.
Il protocollo RTS/CTS (Request To Send/Clear to Send) è stato disegnato per prevenire le collisioni quando si verificano situazioni di "nodi nascosti". Un RTS/CTS definisce la dimensione massima del frame di dati che è possibile trasmettere prima che la prossima richiesta RTS/CTS sia inoltrata. Quando un frame di dati supera il valore di RTS/CTS impostato (tra 0 e 2432 bytes), la stazione che vuole trasmettere deve inviare un messaggio RTS all' Access Point per ottenere il permesso ad iniziare.

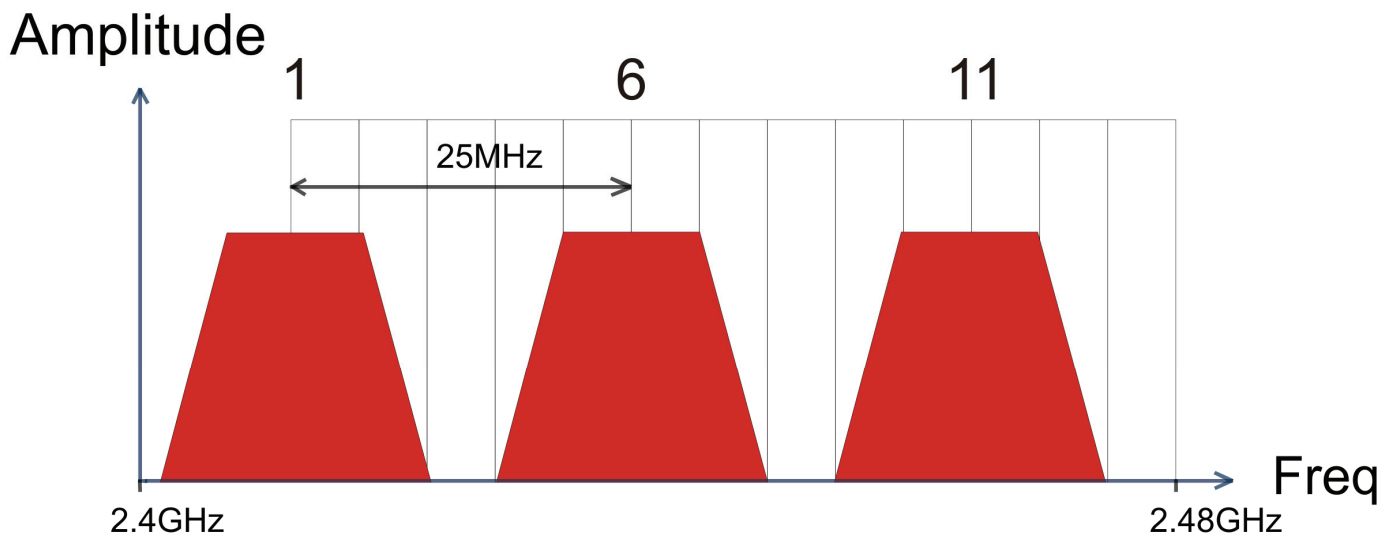
L'Access Point invia quindi a tutte le altre stazioni della rete Wireless un messaggio CTS vietando loro la trasmissione di dati.
A questo punto, il nodo ricevente, dopo aver controllato l'integrità dei dati ricevuti (a tal fine viene utilizzato una sorta di CRC) invia un messaggio di ACK per informare il trasmittente dell'avvenuta corretta ricezione del pacchetto.

L'utilizzo di questo protocollo unito all'invio di ACK (segnalazione di corretta ricezione di un frame) di corretta ricezione ed al traffico di gestione e controllo comporta un importante overhead che riduce, in maniera sensibile, il throughput massimo ottenibile.

Canali

Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11b/g è suddiviso in "canali". Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point vicini.
L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap".
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6).

Ogni canale occupa all'incirca 22Mhz, essendo l'intera banda ISM di 80Mhz possono essere utilizzati contemporaneamente soltanto 3 dei 13 canali disponibili.

Il disegno seguente illustra meglio quanto detto:

Utilizzando un quarto AP questo andrebbe a creare fenomeni di overlapping (sovrapposizione spettrale) generando un drastico deterioramento delle prestazioni.

Modalità Operative

Lo standard integra 2 differenti modalità operative:

- Infrastructure: in questa modalità i differenti client si contendono il mezzo radio e quindi ai servizi messi a disposizione dalla rete. La gestione delle contese è affidata ad un'entità centralizzata che prende il nome di Punto d'Accesso. Con l'uso di algoritmi di sicurezza l'AP può anche essere responsabile dell'autenticazione dei client e cifratura del traffico.
- Ad Hoc: in questa modalità non è presente un AP ma soltanto una moltitudine di client che devono essere configurati con lo stesso SSSID, lo stesso canale, in modalità Ad-Hoc e con la stessa chiave WEP. Lo standard non prevede che la velocità di connessione sia superiore ad 11Mbps.

APPENDICE F: Sicurezza nel Wireless

Per la natura stessa delle reti wireless tutta una nuova serie di considerazioni sulla sicurezza vanno affrontate. Il segnale radio può infatti essere intercettato da terzi non autorizzati che potrebbero cercare di estrarne informazioni preziose.
Sino ad oggi la sicurezza nelle reti WLAN è stata garantita dal protocollo WEP(Wired Equivalent Privacy) a 64/128. Purtroppo:

- le vulnerabilità WEP protocollo e la non facilità del contenimento del segnale wireless
- disattese aspettative di throughput

hanno generato, in taluni utenti, una certa diffidenza nei confronti della Tecnologia Wireless.
Per cercare di colmare alle lacune della sicurezza Wireless la IEEE sta sviluppando un nuovo standard, chiamato IEEE802.11i, che permetterà di rendere le reti wireless finalmente affidabili.
In attesa delle ratifica di questo standard la Wi-Fi Alliance ha derivato dalla versione preliminare un insieme si specifiche che va sotto il nome di WPA (Wi-Fi Protected Access).

Come opera il WEP

Il segnale radio, come già evidenziato in precedenza, è di difficile contenimento è può pertanto essere intercettato da utenti non autorizzati (è sufficiente che abbiano un comune client wireless in standard IEEE802.11b/g).
Il protocollo WEP nasce per limitare questo fenomeno.
Nel dettaglio i servizi offerti dal WEP sono:

- autenticazione delle stazioni che accedono ai servizi di rete
- integrità dei dati trasmessi sul canale radio (nessuna cambiamento è possibile senza che il sistema non se ne accorga)
- riservatezza dei dati trasmessi sul canale radio (nessuno può comprendere l’informazione contenuta nei pacchetti che sono cifrati con l’algoritmo RC4)

Le principali critiche mosse al WEP sono le seguenti:

- Una sola chiave segreta è utilizzata per l’autenticazione (di fatto non si autentica un client, al massimo si sa che il client appartiene al gruppo di utenti autorizzati)
- Un client che conosce la chiave può intercettare tutto il traffico scambiato dagli altri client wireless.

- La chiave di autenticazione è statica ed è usata anche per la cifratura (un attaccante può cercare di entrare nel sistema decifrando il traffico dati che contiene questa chiave)
- Debolezza nel modo con cui il WEP costruisce la chiave di cifratura (diversa ogni trama) coi cui l'RC4 cifra il messaggio
- Debole contro attacchi di integrità o che sfruttano la mancanza di autenticazione di ogni messaggio

Come opera il WPA (in modalità PSK e 802.11x)
In attesa delle ratifica dello standard IEEE802.11i la Wi-Fi Alliance ha derivato dalla versione preliminare un insieme di specifiche che va sotto il nome di WPA (Wi-Fi Protected Access).
Le caratteristiche peculiari del WPA sono:

- Integrazione del TKIP (Temporal Key Integrity Protocol) per permettere il cambio della chiave e migliora il controllo di integrità dei pacchetti
- Meccanismo avanzato per gestire l'autenticazione e il controllo degli accessi ai servizi di rete in modo centralizzato (802.11x tramite EAP, l'uso di TLS è obbligatorio)
- La chiave di autenticazione è diversa da quella utilizzata per la cifratura (che grazie al TKIP cambia continuamente)
- Permette l'autenticazione direttamente sull'AP (WPA-PSK)

Cosa prevede il futuro (WPA2)
Approvato di recente dalla Wi-Fi Alliance, il nuovo standard WPA2 è l'evoluzione del primo WPA (Wi-Fi Protected Access) che è oggi supportato dalla maggior parte degli apparati compatibili IEEE802.11g.
Lo standard WPA, richiesto prepotentemente dal mercato per porre fine alla debolezza intrinseca del WEP, ha purtroppo tratto dall'802.11i solo una parte delle specifiche.
Il nuovo WPA2 invece abbracciando pienamente l'IEEE802.11i ha necessariamente introdotto il supporto per l'Advanced Encryption Standard (AES), protocollo di cifrature utilizzato già da tempo nelle VPN IPSec.
I dispositivi WPA2 saranno compatibili con quelli WPA che però dovranno essere riaggiornati tramite il rilascio di nuovi firmware e/o driver. Il problema risiede nella capacità di calcolo (richiesta dall'AES) che rischierebbe di essere praticamente troppo elevata per gli apparati oggi in commercio.

Ogni sistema di cifratura dati è basato su password.

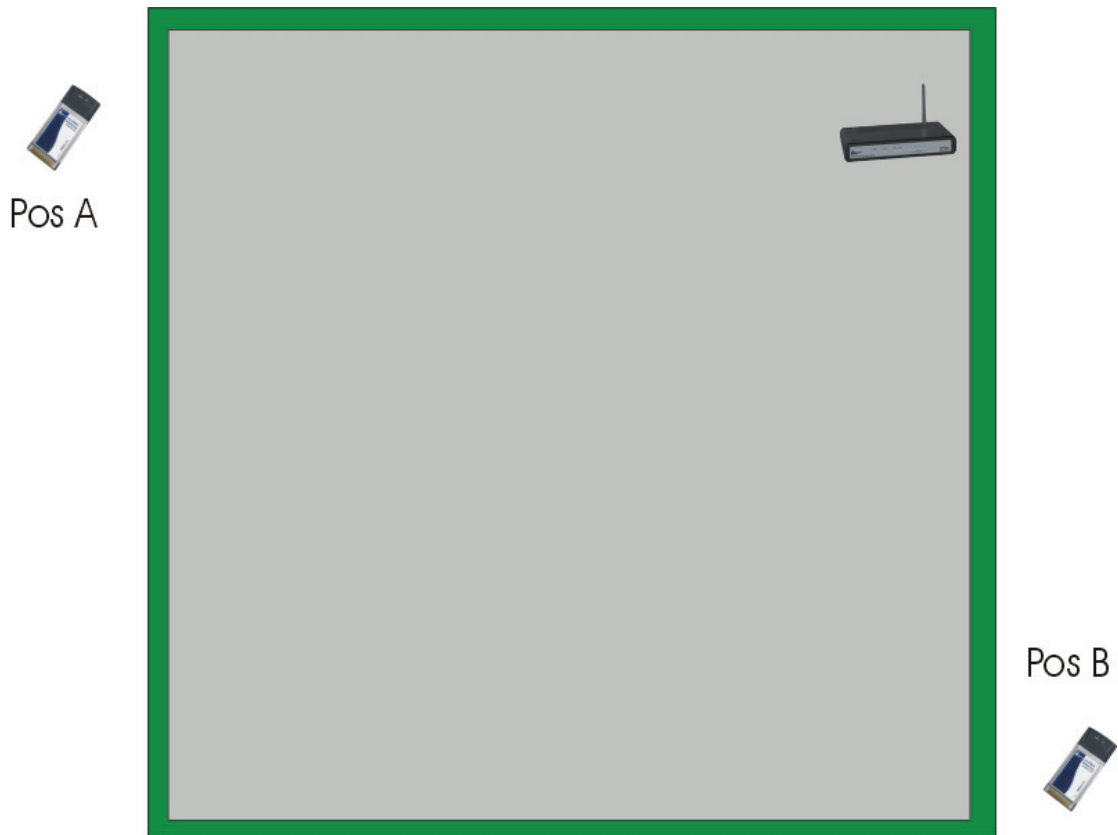
Queste possono essere lunghe, nel caso del WPA in PSK, da 8 sino a 63 caratteri.

Più lunga è la password e meno ha senso compiuto (usare caratteri alfanumerici, numeri e punteggiatura di ogni genere) più questa risulterà sicura.

APPENDICE G: Copertura

Considerazioni Generali

In condizioni ideali la copertura offerta dal dispositivo può arrivare anche a coprire diverse decine di metri. E' però opportuno considerare che pareti divisorie attenuano fortemente il segnale. Oggetti metallici riflettono le onde elettromagnetiche e possono generare (al pari di particolari ambienti indoor) fastidiosi cammini multipli. Non va trascurato inoltre il fenomeno dell'interferenza con altri apparati operanti sulle frequenze vicine.
Rispettare i seguenti punti per massimizzare la copertura offerta dal dispositivo.

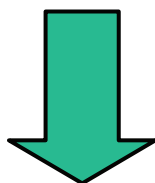
- Ogni muro attenua il segnale, posizionare il dispositivo in un luogo appropriato al fine di minimizzare il numero di muri attraversati dal segnale.
- Porte o ampie superfici metalliche non sono attraversate dalla propagazione elettromagnetica. E' bene prendere in considerazione questo fatto.
- Allontanare l'AP Wireless da ogni altro dispositivo che produca emissioni RF.
- Nel posizionamento dei vari client considerare una linea che idealmente unisce il Wireless AP col client in questione (NetCamera NVW). Se tale linea intersecherà dei muri (caso assai frequente), cercare di minimizzare la superficie attraversata (per evitare di avere un'attenuazione importante). Si veda la figura sottostante:

Il Client in posizione B avrà un’enorme attenuazione e peggiori prestazioni che non il client in posizione A, benché la distanza effettiva dall’AP sia quasi identica nei 2 casi. E’ sufficiente collocare il Wireless AP al centro del locale per migliorare decisamente le prestazione del client B, senza per questo peggiorare le prestazioni del client A.

Dove installare un AP

Si deve operare sulla diminuzione 2 fattori:

- Distanza media
- Sezioni di muro attraversate

E’ decisamente meglio avere una rete i cui client abbiano un link mediamente buono che non una rete con taluni client con link eccellente ed altri con link molto scarso.

La stazione lontana, che generalmente trasmette con un data rate più basso, tende a consumare un «airtime» elevato.

L’AP ha meno tempo da dedicare a client più vicini e più veloci.

Prestazioni complessivi peggiori.

APPENDICE H: Considerazioni sulla Salute

Quando un organismo è immerso in un campo elettromagnetico avviene un'interazione nota come "effetto biologico". Non bisogna necessariamente associare all'"effetto biologico" un danno. Il problema può sorgere quando tale effetto supera la capacità di compensazione dell'organismo.
E' opportuno considerare che il livello di emissioni di un dispositivo wireless conforme alle direttive stabilite dall'IEEE (Institute of Electrical and Electronic Engineers) è notevolmente inferiore all'emissione generata da dispositivi di uso comune.
Un comune terminale GSM emette infatti una potenza che può arrivare e superare i 600mw, mentre un apparato UMTS emette una potenza del 20% inferiore.
A titolo di confronto un apparato Wireless difficilmente supera, in condizione di uso normale, i 17 dBm (circa 50mW) essendo di fatto oltre un ordine di grandezza inferiore.
Già queste considerazioni puramente energetiche dovrebbero tranquillizzare circa ogni eventuale dubbio.
Va inoltre considerato che l'uso del cellulare avviene ad una distanza tipica di qualche centimetro e dunque, essendo l'antenna di tipo isotropica, metà della potenza trasmessa attraversa la testa dell'utilizzatore e crea un effetto "riscaldamento" avvertibile soprattutto nei tessuti superficiali.
Nel caso di un apparato wireless possono presentarsi 2 casi diversi:

- Antenna isotropica: va considerato l'angolo solido con cui questa viene vista (generalmente qualche grado)
- Antenna direttiva: emette potenza solo nella zona di direttività

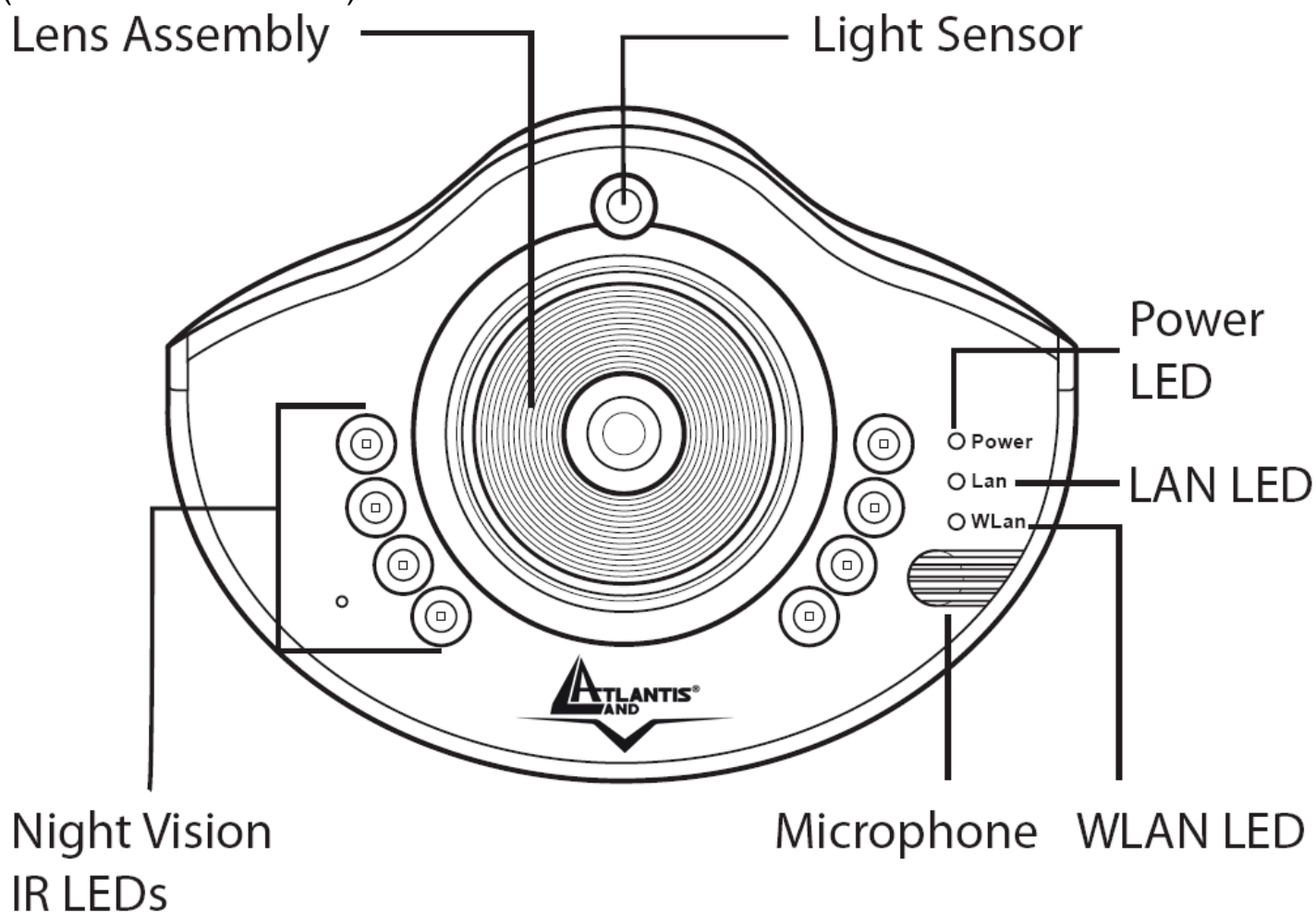
In entrambi i casi l'energia che arriva all'utilizzatore va da una frazione di quella trasmessa (e non la metà come nel caso del cellulare) sino ad arrivare a zero nel caso di antenna direttiva.
In tabella un grafico comparativo di quanto sin qui detto:

Apparato	Potenza Emessa	Angolo di Visuale	Potenza Effettiva
Wireless IEEE802.11b/g	**50mW**	**1/15**	**<5mW**
Cellulare GSM	**600mW**	**1/2**	**Circa 300mW**
Cellulare UMTS	**500mW**	**1/2**	**Circa 250mW**

Il Decreto del 20 Giugno 1995, n.458 (Legge Cautelativa dello Stato) impone di usare il telefonino tenendo l'antenna ad almeno 20cm da qualsiasi parte del proprio corpo.

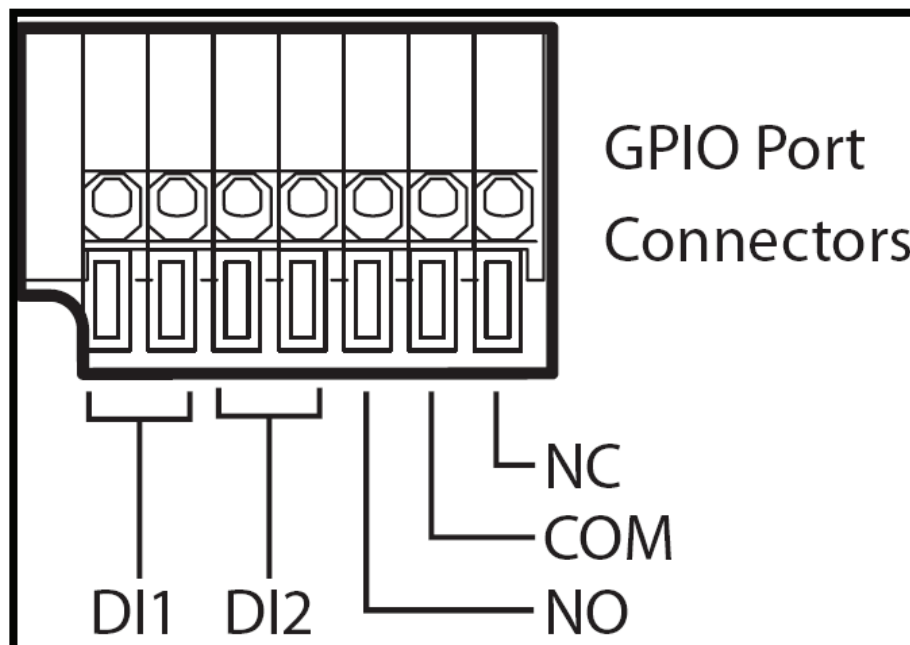
Ad oggi, tutti gli studi effettuati hanno concluso che non esistono effetti termico-biologici pericolosi, a patto di rispettare le norme ETSI sull'emissione.

APPENDICE I: Messa a Fuoco

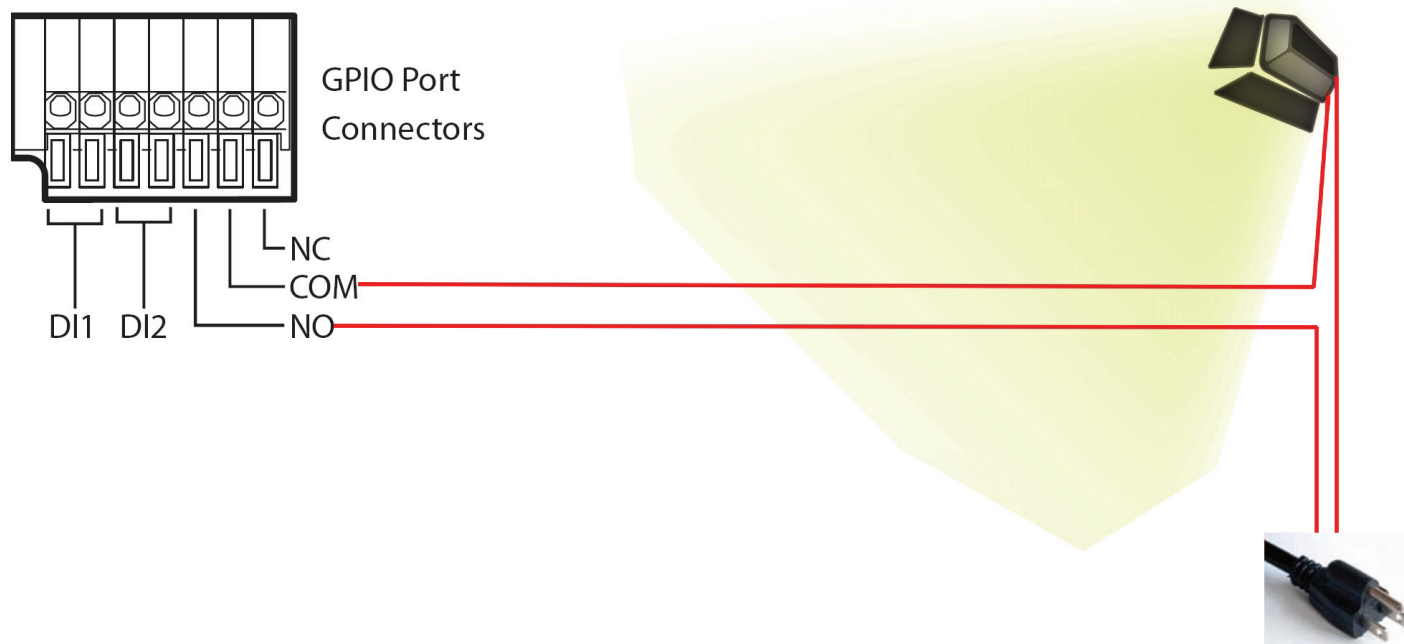
La messa a fuoco della NetCamera NVW aiuta ad ottenere un'immagine a video migliore. E' possibile migliorare la messa a fuoco operando direttamente sulla lente (ruotare delicatamente).

E' inoltre possible operare sui parametri di visualizzazione dell'immagine anche accedendo direttamente alla sezione Setup->Basic->Video.

Non esporre mai la lente direttamente ai raggi solari, questo potrebbe danneggiare il dispositivo.
Il dispositivo è stato disegnato per un utilizzo indoor.

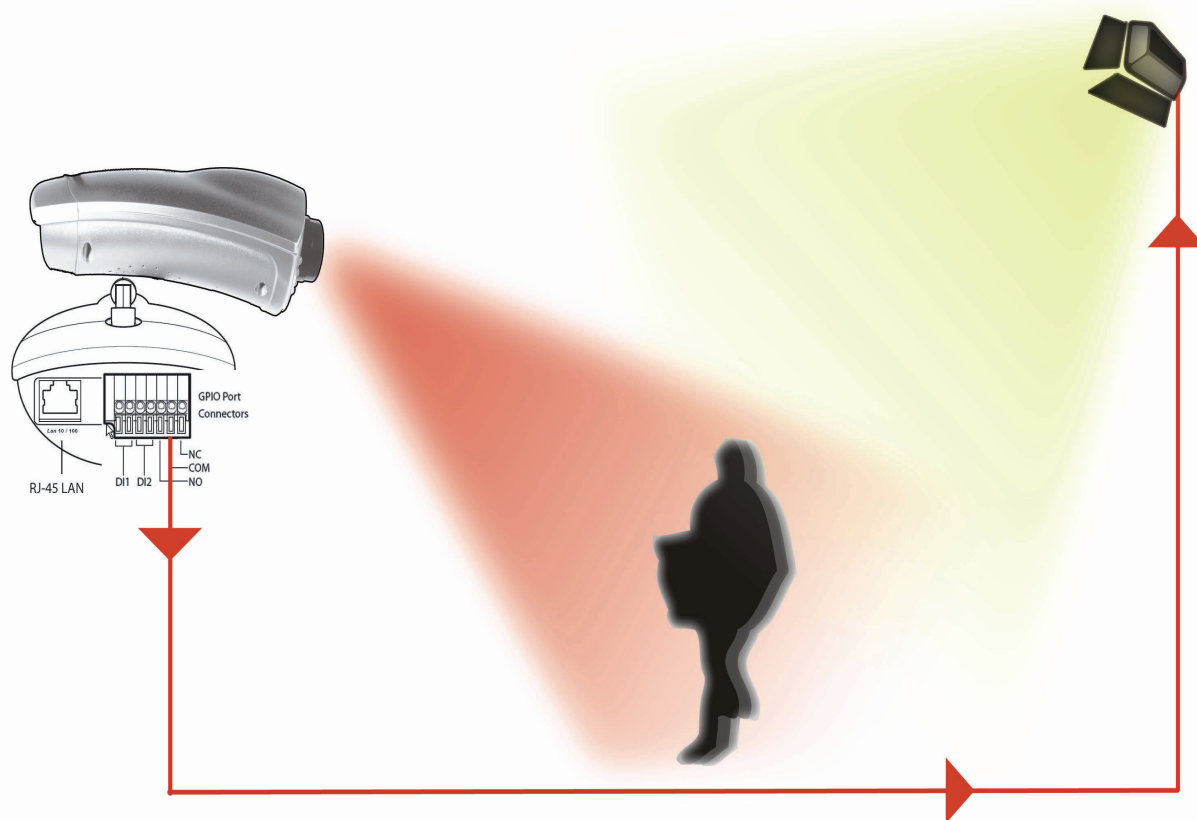
APPENDICE L: GPIO

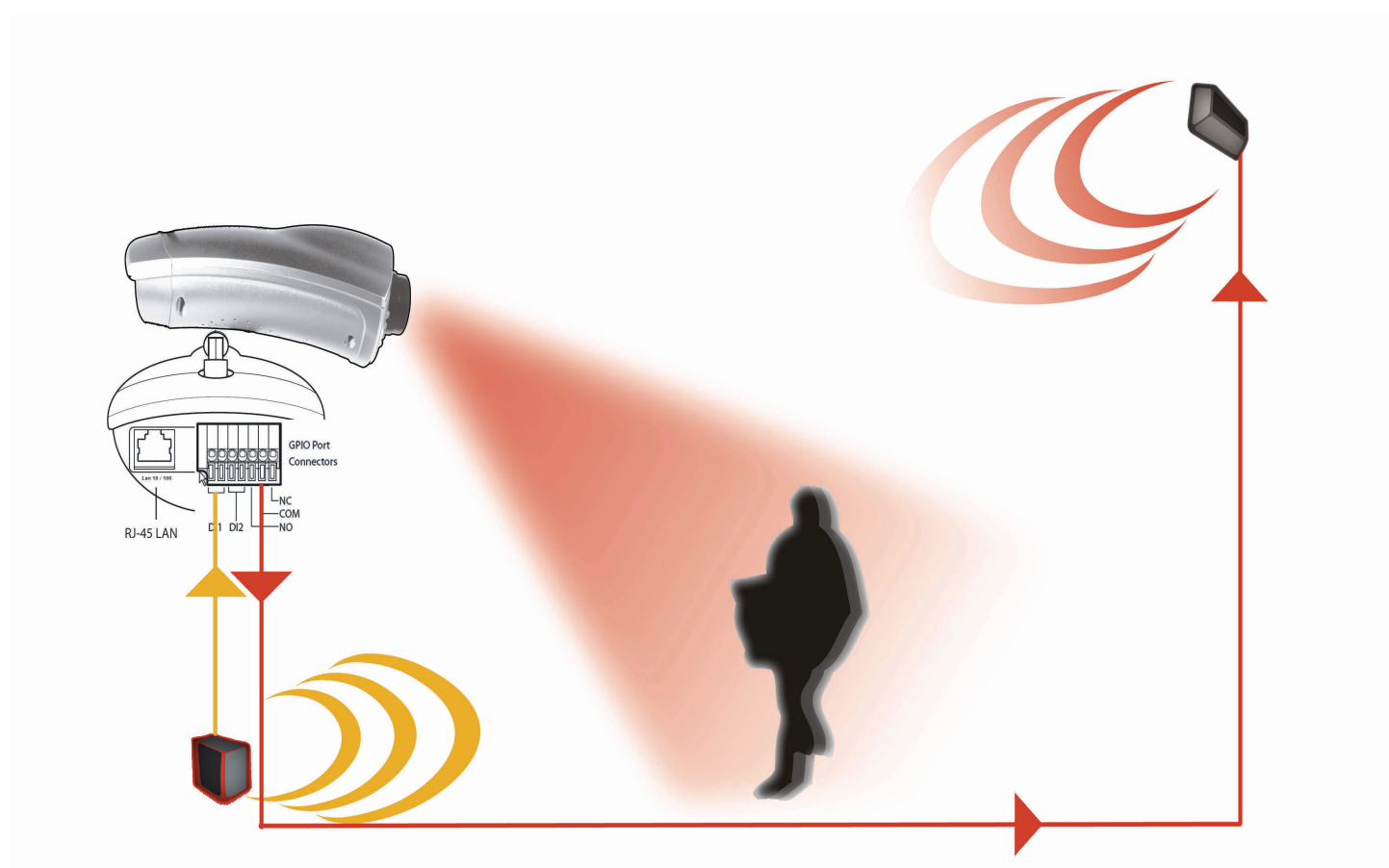
La serie NetCamera NV /NVW integra avanzate funzioni di commutazione (2x DI in ingresso, 1x DO in uscita) che rendono possibili la ricezione/invio di segnali ad altri dispositivi di allarme (rilevatori volumetrici, PIR o sirene).
Il DO è di fatto un interruttore il cui stato è controllato dal sistema operativo della telecamera (rilevazione del movimento e/o da un DI collegato ad un altro apparato d'allarme) e può essere collegato ad un faro e/o sirena e controllarne l'azionamento/spegnimento.
In Figura è possibile avere un dettaglio delle porte DI/DO presenti nel retro dell'apparato.

Nella tabella seguente è possibile avere un quadro dello stato logico degli interruttori controllati e di cosa generi un Trigger.
Ad esempio se si utilizza NO/COM l'interruttore è aperto, mentre l'evento trigger ne cambia lo stato chiudendolo.
Analogamente NC/COM è normalmente chiuso, mentre l'evento trigger ne cambia lo stato aprendolo.

NO-normal opened	Trigged
NC-normal closed	Trigged

In figura è possibile osservare un esempio in cui si collega il dispositivo ad una lampada. Si è utilizzato il DO in modalità NO (circuito aperto) pertanto la lampada sarà spenta. Attivando un trigger (ad esempio col Motion Detection) la lampada verrà accesa perché il DO diverrà un circuito chiuso.

E' opportuno rispettare le seguente regole di dimensionamento del DO:
Max 24VDC/1A
Max 125VAC /0.5A

Esempi di Funzioni di Commutazione (DO)

In figura è possibile osservare la telecamera che tramite il DO controlla una sirena/spot. Quando l'intruso viene rilevato dal dispositivo (che ha la funzionalità Motion Detection attiva) la telecamera può inviare via mail/ftp la foto e pilotare l'accensione di un dispositivo esterno quale una sirena e/o spot per mettere in fuga l'intruso.

Esempi di Funzioni di Commutazione (DO e DI)

In figura è possibile osservare un'installazione in cui un dispositivo esterno (rilevatore di movimento, in giallo), collegato su una porta DI, pilota tramite DO l'accensione di una sirena. La funzionalità di Motion Detection attivata permetterà alla telecamera di inviare una foto chiara ad un indirizzo FTP/Mail.

APPENDICE M: Caratteristiche Tecniche

Caratteristiche Tecniche
CMOS Sensor
Number of effective pixels: 307200 pixels (VGA)
Resolution: 640 x 480 pixel
Lens Type: C3 Mount Lens (removable)
Focal length: f=6.0mm
F-number: F1.8
Focus Extent: 20 cm - ∞

Image (Video Setting)
Image compression: MPEG4
Frame rate: 30fps@QVGA, 30fps@VGA
Compression Rate selection: 5 levels
Video resolution: 320x240, 640x480
Upside down and Mirror: Yes
Brightness/ Contrast /Saturation/HUE
Night Vision: 8 x IR LEDs (auto/manual)

Audio
MIC Input: Internal MIC (mono)
Audio Compression: ADPCM 16/24/32/40 Kbit

Hardware Interface
LAN Connector: One RJ-45 port to connect to 10/100Mbps Ethernet, auto-sensed
WLAN: one 2.2 dBi Antenna built-In (IEEE802.11g with WEP 65/128 and WPA* support)
LED Indicator: Power LED, LAN, WLan
Power Supply: DC 5V, switching type
GPIO: 2 x Sensor IN / 1 x Sensor OUT

Communication Support
Communication: 10/100Mbps Ethernet
Communication protocol: HTTP, TCP/IP, UDP, ARP, ICMP,DHCP, PPPoE, DDNS, DNS, FTP

System
CPU: ARM9/MPEG4 encode chip (VGA)

System Requirements
Local Area Network: 10Base-T Ethernet or 100Base TX Fast Ethernet
CPU: Intel Celeron 1.5GHz or above (Intel Pentium 4 is preferred)
Memory Size: 128 MB (256 MB recommended)
VGA card resolution: 800x600 or above
Internet Explorer 5.0 or above (ActiveX)

Advanced Features
MPEG4 encode Chip
Hardware motion detection and send e-mail (with snap shot) when motion detected
GPIO: Sensor IN, Alarm Out
Single Frame Image Snap shot (manual)
Record (AVI, manual)
FTP / PPPoE / Dynamic DNS Clients

Operating environment
Operating temperature: 5°C ~ 30°C
Storage temperature: -25°C ~ 50°C
Humidity: 20% ~ 80% non-condensing

Package Contents:
One IP Security Wireless Night Vision Camera
One Quick Installation Guide
One Installation CDRom
One Metal Clip (wall mounting)
One DC Power Adapter
One RJ-45 Ethernet Cable

Specifications are subjected to change without prior notice. No liability for technical errors and/or omissions
Performance and Throughput are influenced by many factors (interference, noise, environments)
*available with new firmware release

Atlantis Land S.p.A.
Viale De Gasperi, 122
Mazzo di Rho – MI – Italy
info@atlantis-land.com
sales@atlantis-land.com

Where solutions begin